2019-04-30

Volume I Acquisition Research Creating Synergy for Informed Change, Wednesday Proceedings

NPS Acquisition Research Program

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/63015

SYM-AM-19-058

Proceedings
of the
Sixteenth Annual Acquisition Research Symposium

Wednesday Sessions
Volume I

Acquisition Research:
Creating Synergy for Informed Change

May 8–9, 2019

Published: April 30, 2019

Approved for public release; distribution is unlimited.

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Table of Contents

SYM-AM-19-029

Proceedings
Of the
Sixteenth Annual Acquisition Research Symposium

Wednesday Sessions
Volume I

Acquisition Research:
Creating Synergy for Informed Change

May 8–9, 2019

Published: April 30, 2019

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

THIS PAGE INTENTIONALLY LEFT BLANK

Welcome: Dr. Robert (Bob) Mortlock, Principal Investigator, Acquisition Research Program

Dr. Robert Mortlock, PhD, CMBA, PMP, PE, COL USA (Ret), — Dr. Mortlock is the Principal Investigator, Acquisition Research Program, Naval Postgraduate School, managed defense systems development and acquisition efforts for the last 15 of his 27 years in the U.S. Army, culminating in his assignment as the project manager for Soldier Protection and Individual Equipment in the Program Executive Office for Soldier. He retired in September 2015 and now teaches defense acquisition and program management in the Graduate School of Business and Public Policy at the Naval Postgraduate School in Monterey, California. He holds a Ph.D. in chemical engineering from the University of California, Berkeley, an MBA from Webster University, an M.S. in national resource strategy from the Industrial College of the Armed Forces and a B.S. in chemical engineering from Lehigh University. He is also a recent graduate from the Post-Doctoral Bridge Program of the University of Florida’s Hough Graduate School of Business, with a management specialization. He holds DAWIA Level III certifications in program management (PM), test & evaluation (T&E), and systems planning, research, development & engineering (SPRDE).

Keynote Speaker: Dyke D. Weatherington, Deputy Assistant Secretary of Defense, Information & Integration Portfolio Management

Mr. Dyke Weatherington is the Deputy Assistant Secretary of Defense, Information & Integration Portfolio Management (I&IPM), Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), Pentagon, Washington, D.C. He manages and is responsible for acquisition shaping, analysis and oversight of warfighter capability portfolios across the Department in the nuclear weapons systems; nuclear command, control, and communications; missile defense; cyber; and space domains. He leads assessments of cost, schedule, and performance risks of acquisition programs, and works directly with the Services, the Intelligence Community, and the Office of the Under Secretary of Defense for Research and Engineering to address identified gaps in program strategies. His DoD portfolio includes Ground Based Strategic Deterrence, Long Range Stand-Off weapon, GPS Enterprise, Space Launch, Space Control, Missile Defense, and cyber enabling programs. His Intelligence Community portfolio includes major system acquisition programs of the National Reconnaissance Office, National Geo-Spatial Intelligence Agency, National Security Agency, and Defense Intelligence Agency. He serves as the I&IPM Senior Acquisition Officer and the primary liaison between Joint Staff, Services, Agencies, and Congress, facilitating actions to achieve cost, schedule, and performance goals and advising the Milestone Decision Authority on program acquisition decisions.

Mr. Weatherington's prior duties included Deputy Director, Intelligence, Surveillance and Reconnaissance in OUSD(A&S), Space, Strategic and Intelligence Systems (SSI). Mr. Weatherington was also the OUSD(AT&L) functional lead for the Defense Space Council. Prior to his assignment to SSI, Mr. Weatherington was the Deputy Director, Unmanned Warfare and ISR, Strategic & Tactical Systems.

Mr. Weatherington holds a Bachelor of Science degree in engineering mechanics from the United States Air Force Academy (1981) and a Master of Arts in National Securities Studies from California State University (1993). He is also a graduate of the Air Force Air Command and Staff College and the Defense Systems Management College. He has been awarded numerous OSD and Air Force decorations including the Airman's Medal, OUSD Exceptional Civilian Service Award, and FY17 Presidential Rank Award.

Mr. Weatherington was born and raised on his family's farm near Burnside, Illinois, and is married with four children. He resides with his family in Northern Virginia.

Panel 1. Middle-Tier Acquisition and the 2018 National Defense Strategy

Wednesday, May 8, 2019	
9:05 a.m. – 10:15 am.	**Chair: Hon. David Berteau**, President and CEO, Professional Services Council **Panelists:** **Andrew Hunter**, Director, Defense-Industrial Initiatives Group, and Senior Fellow, International Security Program, Center for Strategic and International Studies **Hon. Katharina McFarland,** Chair of the Army Research and Development Board, National Academies of Science **Hon. William LaPlante**, Senior Vice President and General Manager, The MITRE Corporation **Stan Soloway**, President and CEO, Celero Strategies, LLC ***Defense Acquisition Trends 2019: A Preliminary Look*** Andrew Hunter, Rhys McCormick, Greg Sanders, Center for Strategic and International Studies

Hon. David Berteau—Mr. Berteau is PSC President and CEO, with 400 member companies of all sizes providing federal contract services. Mr. Berteau was ASD for Logistics and Materiel Readiness and served 14 years in the Defense Department, under six defense secretaries. Earlier, Mr. Berteau was at the Center for Strategic and International Studies (CSIS), Syracuse University's National Security Studies Program, and SAIC. He is a Fellow of the National Academy of Public Administration and taught graduate courses for 14 years at the Maxwell School, Georgetown, and the LBJ School.

Andrew Hunter—Mr. Hunter is a senior fellow in the International Security Program and director of the Defense-Industrial Initiatives Group at CSIS. From 2011 to 2014, he served as a senior executive in the Department of Defense, serving first as chief of staff to undersecretaries of defense (AT&L) Ashton B. Carter and Frank Kendall, before directing the Joint Rapid Acquisition Cell. From 2005 to 2011, Mr. Hunter served as a professional staff member of the House Armed Services Committee. Mr. Hunter holds an M.A. degree in applied economics from the Johns Hopkins University and a B.A. in social studies from Harvard University.

Hon. Katharina McFarland—Ms. McFarland is a leading subject-matter expert on government procurement. Her positions include serving on the board of directors of SAIC, serving as Chairman of the Board of Army Research and Development at the National Academies of Science, serves as a Commissioner of the National Security Commission on Artificial Intelligence, and as a Director on the Procurement Round table. She recently retired from her position as Assistant Secretary of Defense (Acquisition) and acting Assistant Secretary of the Army (Acquisition, Logistics & Technology) after nearly thirty years of public as an accredited Materials, Mechanical, Civil and Electronics Engineer. She has received an Honorary Doctoral of Engineering from the University of

Cranfield, United Kingdom; the Presidential Meritorious Executive Rank Award, the Secretary of Defense Medal for Meritorious Civilian Service Award, the Department of the Navy Civilian Tester of the Year Award, and the Navy and United States Marine Corps Commendation Medal for Meritorious Civilian Service. She is DAWIA Level-III-certified in Program Management, Engineering, and Testing as well as having a professional engineer license and having attained her PMP certification.

Hon. William LaPlante—Mr. LaPlante is senior vice president and general manager for The MITRE Corporation, leading MITRE's National Security Sector (MNS). With more than 30 years of experience in defense technology, he is also a commissioner on the congressionally mandated Section 809 Panel for defense acquisition reform. Previously, LaPlante spent three years as assistant secretary of the Air Force for Acquisition, during which time he brought the $43 billion Air Force acquisition enterprise budget into alignment with the Air Force vision and strategy. At MITRE, LaPlante oversees operations of two federally funded research and development centers (FFRDCs)—The National Security Engineering Center (NSEC), and The National Cybersecurity FFRDC. He is accountable for increasing MITRE's strategic value across the company's DoD, intelligence and cybersecurity portfolios.

Stan Soloway—Mr. Soloway is President & CEO of Celero Strategies, LLC, a full-service strategic consultancy focused on the federal market. Prior to founding Celero Strategies in January, 2016, Stan served for 15 years as the President & CEO of the Professional Services Council, the largest and most influential national association of government technology and professional services firms. During the second half of the Clinton Administration, Stan served as the Deputy Undersecretary of Defense and was responsible for wide-ranging reforms to defense acquisition and technology policy and practices, and broader department-wide re-engineering. Stan was awarded both the Secretary of Defense Medal for Exceptional Public Service and the Secretary of Defense Medal for Distinguished Public Service, and received the 2016 Consumer Electronics Show (CES) Government Technology Leadership Award. He was also was named the IT Industry Executive of the Year in 2013 by Government Computer News; is a Fellow of both the National Academy of Public Administration and the National Contract Management Association, a principal at the Partnership for Public Service, and served from 2007 to 2013 as a Senate-confirmed member of the Board of Directors of the Corporation for National and Community Service, the federal agency that oversees AmeriCorps and other national service programs.

Defense Acquisition Trends 2019: A Preliminary Look

Rhys McCormick—is a Fellow with the Defense-Industrial Initiatives Group (DIIG) at the Center for Strategic and International Studies (CSIS). His work focuses on unmanned systems, global defense industrial base issues, and U.S. federal and defense contracting trends. Prior to working at DIIG, he interned at the Abshire-Inamori Leadership Academy at CSIS and the Peacekeeping and Stability Operations Institute at the U.S. Army War College. He holds a bachelor's degree in security and risk analysis from Pennsylvania State University and a master's degree in security studies from Georgetown University. [rmccormick@csis.org]

Greg Sanders—is a Fellow in the International Security Program and Deputy Director of the Defense-Industrial Initiatives Group at CSIS, where he manages a research team that analyzes data on U.S. government contract spending and other budget and acquisition issues. In support of these goals, he employs SQL Server, as well as the statistical programming language R. Sanders holds a master's degree in international studies from the University of Denver, and he holds a bachelor's degree in government and politics and a bachelor's degree in computer science from the University of Maryland. [gsanders@csis.org]

Andrew Hunter—is a senior fellow in the International Security Program and director of the Defense-Industrial Initiatives Group at CSIS. From 2011 to 2014, he served as a senior executive in the Department of Defense, serving first as chief of staff to Under Secretaries of Defense (AT&L) Ashton B. Carter and Frank Kendall, before directing the Joint Rapid Acquisition Cell. From 2005 to 2011, Hunter served as a professional staff member of the House Armed Services Committee. Hunter holds an MA degree in applied economics from the Johns Hopkins University and a BA in social studies from Harvard University. [ahunter@csis.org]

Abstract

This paper presents a preliminary look at the Fiscal Year (FY) 2018 Department of Defense (DoD) contracting trends available in the Federal Procurement Data System (FPDS). This year's study focuses on the defense acquisition's systems response to the 2018 National Defense Strategy's emphasis on peer and near-peer competition, forging a new relationship between the DoD and the National Security Innovation Base, and the need for increased investment in emerging technologies. In particular, this report looks at whether there has been a significant shift in the DoD's investment posture between equipment (Products) and research and development. Additionally, this report includes analysis of the topline DoD contracting trends.

Introduction

This paper presents a preliminary look at the Fiscal Year (FY) 2018 Department of Defense (DoD) contracting trends available in the Federal Procurement Data System (FPDS). The FY 2018 DoD contract data provides critical insights into the defense acquisition system's response to the 2018 National Defense Strategy and new administration priorities (DoD, 2018). Last year, the FY 2017 DoD contract data show that although DoD contract spending has rebounded between FY 2015 and FY 2017, the growth has been largely concentrated amongst existing product lines over research and development or services. Given previous NPS-funded research showing that it often takes two years for the contract data to reflect acquisition reforms or changes in priorities, the FY 2018 contract data can illuminate whether the administration's priorities are better reflected in its second year (McCormick et al., 2015).

This report uses the methodology used in Center for Strategic and International Studies (CSIS) reports on federal contracting. For over a decade, the Defense-Industrial Initiatives Group (DIIG) has issued a series of analytical reports on federal contract spending for national security by the government. These reports are built on FPDS data, which is downloaded in bulk from USAspending.gov. DIIG now maintains its own database of federal spending that includes data from 1990–2018. This database is a composite of FPDS and DD350 data. For this report, the study team relied on FY 2000–FY 2018 data. All dollar figures are in constant FY 2019 dollars, using the latest Office of Management and Budget (OMB) deflators. For additional information about the CSIS contracting data analysis methodology, see https://github.com/CSISdefense/Lookup-Tables.

For this paper, CSIS focused on the following research questions:

- Area: Has there been a significant shift in the DoD's investment between products, services, and research and development (R&D) to reflect the 2018 National Defense Strategy priorities?
- Platform Portfolio: Have there been significant changes across the different sectors of the defense industrial base?
- R&D: Has the DoD started to recover from its trough in the development pipeline for major weapon systems?
- Composition of the Industrial Base: What has the defense contracting rebound meant for the composition of the defense industrial base? What has it meant for vendors of different sizes? Has the number of prime vendors and new entrants doing business with the DoD continued to decline?
- Other Transaction Authorities (OTA): What are the significant trends in OTA usage across the DoD?
- Components: Have there been significant shifts in defense contracting trends between the major DoD components?

DoD Contract Spending in a Budgetary Context

The defense contracting rebound that began in FY 2016 continued into FY 2018. As shown in Figure 1, total defense contract obligations increased from $331.1 billion in FY 2017 to $364.5 billion in FY 2018, a 10% increase. Over the last three years, defense contract obligations grew 25% between FY 2015 and FY 2018.

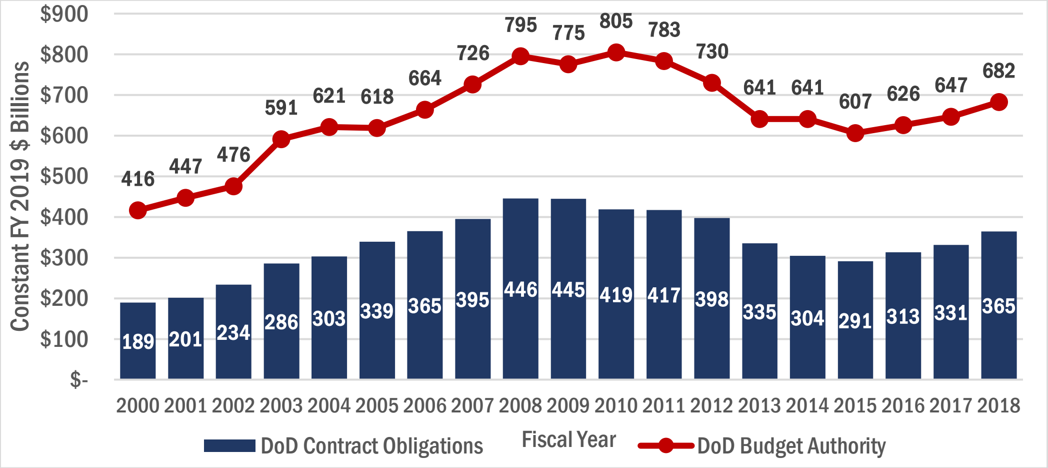


Figure 1. **Defense Contract Obligations vs. Budget Authority, 2000–2018**

Note. Sources: FPDS; DoD, *National Defense Budget Estimates for Fiscal Year 2019 (Green Book)*, Office of the Under Secretary of Defense (Comptroller), April 2018; DoD, *Defense Budget Overview: United States Department of Defense Fiscal Year 2020 Budget Request*, Office of the Under Secretary of Defense (Comptroller/Chief Financial Officer) (March 2019); CSIS analysis.

What Is the DoD Buying?

Despite the 2018 National Defense Strategy (NDS) emphasizing modernization priorities, there has not yet been a significant shift toward NDS-related technology in the DoD's investment posture. During the first two years of the defense contracting rebound, defense contract obligations for products significantly outpaced both services and R&D. In FY 2018, services caught up to products, as defense services and products contract obligations increased 10% and 11%, respectively, a rate in-line with total defense contract obligations growth. Meanwhile, defense R&D contract obligations only increased 4%, well below the 10% increase in total defense contract obligations. As a result, R&D fell to its lowest share of defense contract obligations this century.

Looking at total growth over the course of the defense contracting rebound, defense products contract obligations are up 35% over the last three years. Comparatively, defense services contract obligations increased 17% between FY 2015 and FY 2018, while R&D contract obligations increased just 10% over that same period.

Figure 2 shows defense contract obligations by area from FY 2000 to FY 2018.

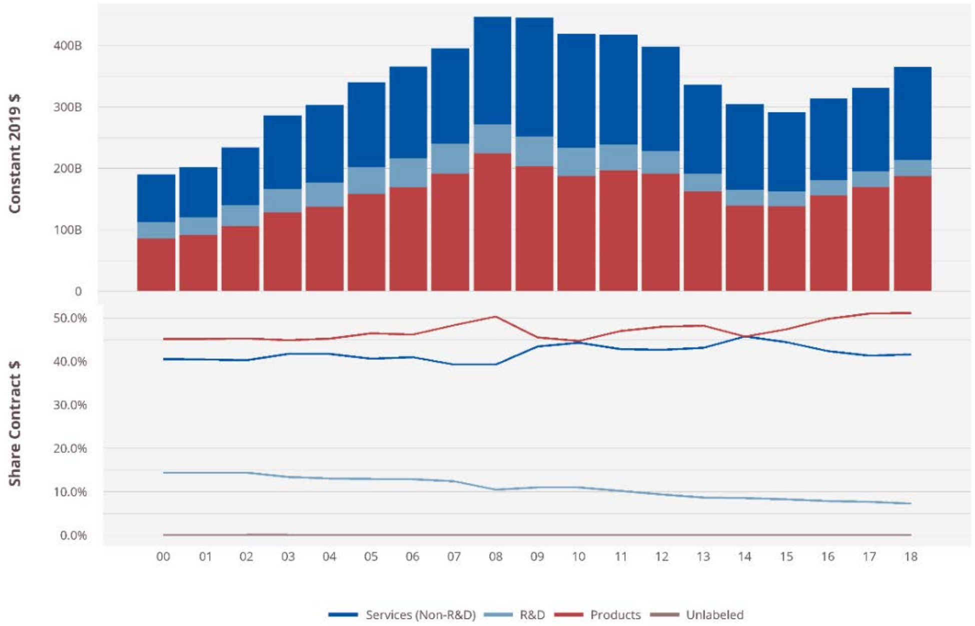


Figure 2. **Defense Contract Obligations by Area, 2000–2018**
(Source: FPDS; CSIS analysis)

Defense Contract Obligations by Platform Portfolio

While there have not been significant shifts in the DoD's investment between products, services, and R&D, there were more significant changes at the sector level in FY 2018.

Aircraft contract obligations increased the most amongst the eleven platform portfolios during the first year two years of the defense contracting rebound but declined in FY 2018. Between FY 2015 and FY 2017, Aircraft obligations increased 34% (McCormick et al., 2018, p. 9). However, in FY 2018, Aircraft defense contract obligations fell from $88.6 billion in FY 2017 to $84.6 billion, a 5% decline. This decline is not outside the norm, as the Aircraft sector, as previously shown during sequestration and the defense drawdown, has been known to whipsaw between growth and declines (McCormick, Hunter, & Sanders, 2017, p. 23). In total over the course of the defense contracting rebound, Aircraft defense contract obligations have increased 29% since FY 2015, a rate slightly higher than topline growth (25%).

Air & Missile Defense contract obligations increased 53% in FY 2018, continuing the whipsaw this sector has seen throughout the defense contracting rebound (McCormick et al., 2018). Over the last four years, Air & Missile Defense contract obligations rose from $9.97 billion in FY 2015 to $10.49 billion in FY 2016 and fell to $8.92 billion in FY 2017, before rising again to $13.65 billion in FY 2018. Despite the whipsaw, total Air & Missile Defense contract obligations are up 37% since FY 2015.

After several years of declining contracting obligations, the Facilities & Construction sector experienced a large up-tick in FY 2018. Facilities & Construction defense contract obligations increased from $39.5 billion in FY 2017 to $47.3 billion in FY 2018, a 20% increase.

Land Vehicles, the sector heaviest hit by sequestration and the defense drawdown, continued rebounding in FY 2018 (McCormick et al., 2017). Land Vehicles defense contract obligations totaled $12.9 billion in FY 2018, a 51% increase from the $8.5 billion obligated in FY 2017. Between FY 2015 and FY 2018, Land Vehicles defense contract obligations have risen from $7.95 billion to $12.9 billion, a 62% increase.

The Ordnance & Missiles continued to steadily grow in FY 2018, a trend that has been ongoing through the course of the defense contracting rebound. Ordnance & Missiles contract obligations increased 17% in FY 2018, rising from $18.9 billion to $22.2 billion. Since FY 2015, Ordnance & Missiles contract obligations have increased 56%.

Figure 3 shows defense contract obligations by platform portfolio from FY 2000 to FY 2018.

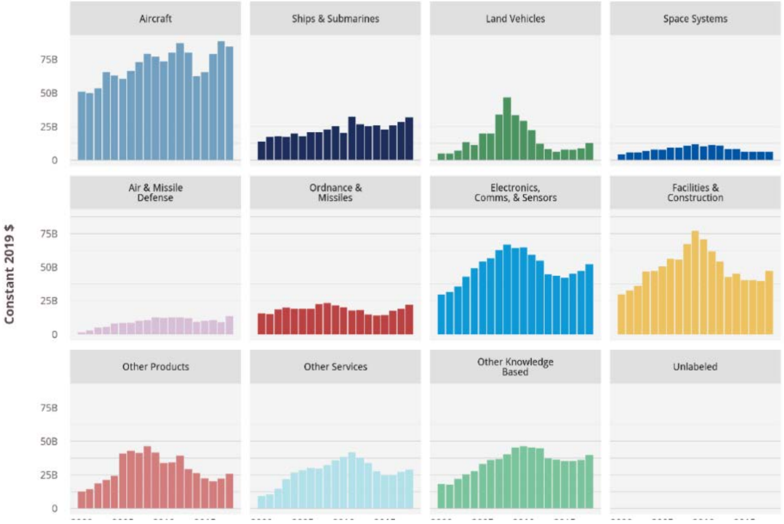


Figure 3. **Defense Contract Obligations by Platform Portfolio, 2000–2018**
(Source: FPDS; CSIS analysis)

Defense Contract Obligations by Stage of R&D

Previous CSIS research showed that in FY 2017, the “seven-year trough in major weapon systems development pipeline appeared to have bottomed out but does still exist in some stages of R&D and it will still be some time before DoD fully recovers” (McCormick et al., 2018, p. 11). The FY 2018 data show that while this largely still holds true, there are notable differences across the different R&D activities.

Figure 4 shows defense contract obligations by stage of R&D from FY 2000 to FY 2018.

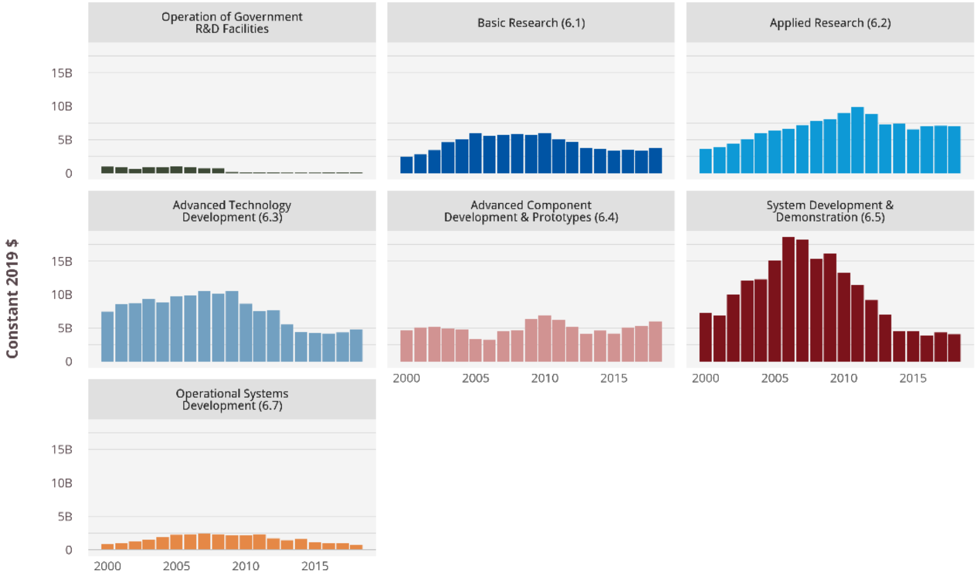


Figure 4. **Defense R&D Contract Obligations, 2000–2018**
(Source: FPDS; CSIS analysis)

The data show that the two earliest stages of R&D, Basic Research (6.1) and Applied Research (6.2), experienced significantly different trends in FY 2018. Defense Basic Research contract obligations increased 11% in FY 2017, a rate nearly three times the rate of the overall growth in defense R&D contract obligations, while Applied Research defense contract obligations declined 1%.

Both the two mid-stage R&D activities, Advanced Technology Development (6.3) and Advanced Component Development & Prototypes (6.4), grew at rates notably above the overall growth in defense R&D contract in FY 2018. Advanced Technology Development defense contract obligations increased from $4.3 billion to $4.8 billion, an 11% increase. Advanced Component Development & Prototypes defense contract obligations increased 14%, rising from $5.3 billion in FY 2017 to $6.0 billion in FY 2018. Of note, as the DoD pushes for increased usage of experimentation and prototyping in the acquisition process, Advanced Component Development & Prototypes accounted for 23% of total defense R&D contract obligations in FY 2018, well above its 14% historical average (McCormick et al., 2019).

After System Development & Demonstration (6.5) contract obligations declined in FY 2018 after having increased in FY 2017, the first year-to-year increase in System Development & Demonstration contract spending since FY 2005. Defense System Development & Demonstration contract obligations fell from $4.33 billion in FY 2017 to $4.06 billion, a 6%. As a share of total defense R&D contract obligations, System Development & Demonstration fell from 17% in FY 2017 to 15% in FY 2018, well below the historical average of 27%.

OTA Usage Across the DoD

OTAs have had a recent resurgence in the DoD thanks in large part to recent legislative changes aimed at incentivizing their usage and the emphasis of acquisition officials in this administration. Previous CSIS research has shown that DoD OTA obligations increased 195% between FY 2015 and FY 2017 (McCormick et al., 2018, p. 14). DoD OTA obligations continued rising in FY 2018, increasing 81% from FY 2017. In total, DoD OTA obligations have increased 352% over the last three years.

As shown in Figure 5, the base and all options (total potential value) of OTA agreements signed in the last few years is increasing at a rate quicker rate than actual OTA obligations. This last year, the total potential value of OTA agreements increased from $11.1 billion in FY 2017 to $26.8 billion in FY 2018, a 138% increase. Since FY 2015, total value of OTA agreements has increased 758% compared to the 352% growth in OTA obligations. Although the DoD will not ultimately exercise all the options contained in these recently signed OTA awards, nor necessarily obligate 100% of the value of even those options that are exercised, there is clearly a widely based increase in the potential scope of OTAs, suggesting that OTA obligations are likely to continue rising in the coming years as these OTAs are executed.

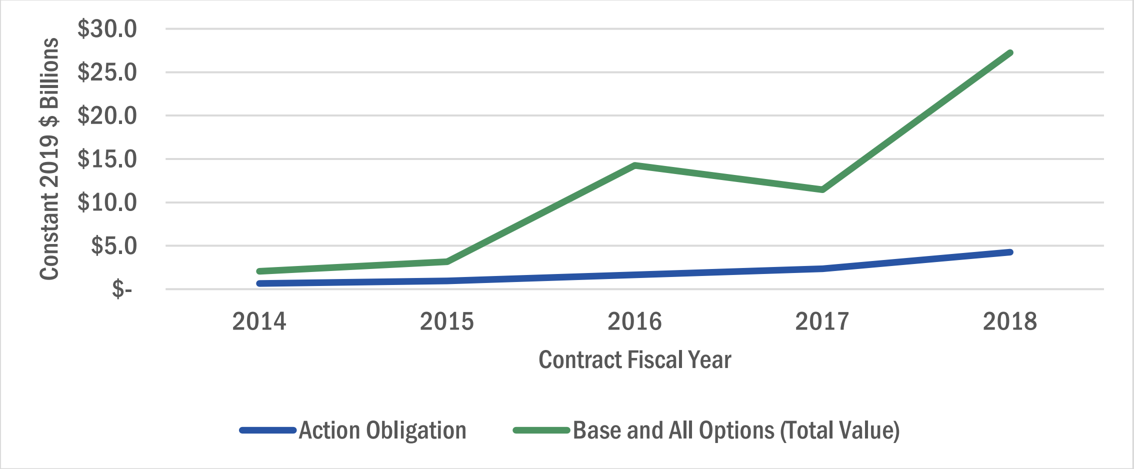


Figure 5. **Defense OTA Obligations vs. Total Value, 2014–2018**
(Source: FPDS; CSIS analysis)

Figure 6 shows defense OTA obligations by customer from FY 2014 to FY 2018.

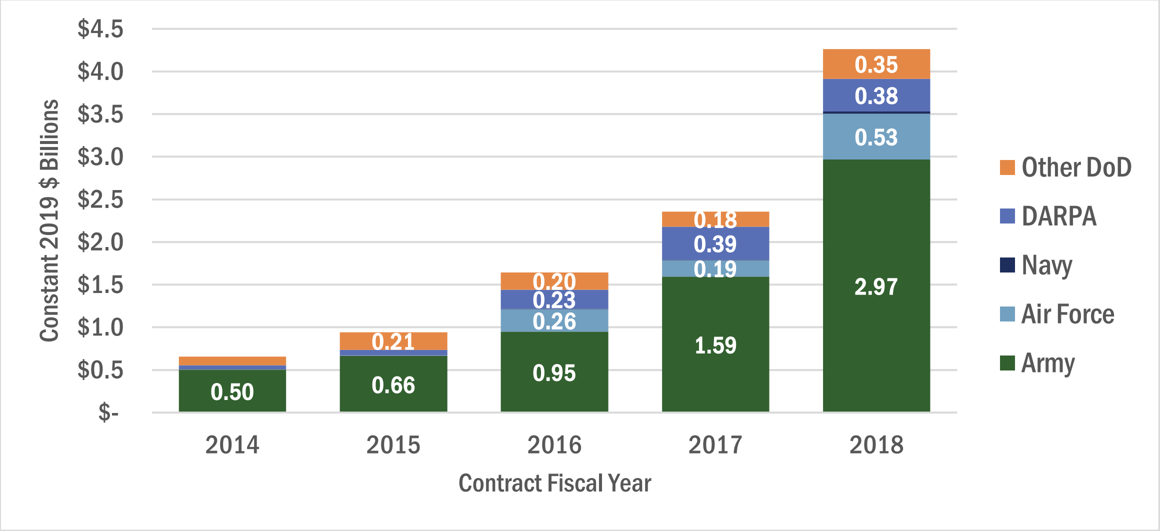


Figure 6. **Defense OTA Obligations by Customer, 2014–2018**
(Source: FPDS; CSIS analysis)

Across the DoD, the Army has been at the forefront of the DoD's OTA resurgence, largely due to its OTA Center of Excellence located at Army Contracting Command New Jersey (ACC-NJ) at Picatinny Arsenal, but over the last year most of the other DoD components substantially increased their usage of OTAs (McCormick et al., 2019, pp. 77–78).

Army OTA obligations increased 86% in FY 2018 and rose as a share of total defense OTA obligations from 68% in FY 2017 to 70%. Over the last three years, Army OTA obligations have increased 348% between FY 2015 and FY 2018.

Prior to the recent legislative changes, the Air Force made some limited use of OTAs, but the service has significantly increased their usage in recent years, particularly this last year. Air Force OTA obligations rose from approximately $0.19 billion in FY 2017 to $0.53 billion in FY 2018, a 176%. Air Force OTA obligations have grown 9982% since FY 2015.

Prior to FY 2018, the Navy accounted for less than 1% of total defense OTA obligations between FY 2015 and FY 2017. While the Navy still makes very limited use of OTAs, it started to make greater usage of them in FY 2018, spending $24.96 million in OTAs in FY 2018 compared to the $7.3 million the service spent in total from FY 2015 to FY 2017.

Composition of the Defense Industry

Defense Contract Obligations by Vendor Size

During the initial two years of the defense contracting rebound, the Big Five fared the best amongst the four vendor size categories, followed by Small and Medium-sized vendors, who grew at rates slightly below the topline growth, while Large vendors fared the worst, declining 1%.[1] However, these trends did not hold true in FY 2018, as the Big Five declined slightly while the other three vendor size categories grew at roughly equal rates.

Defense contract obligations awarded to the Big Five fell from $115.9 billion in FY 2017 to $114.8 billion in FY 2018, a 1% decline. As a share of total defense contract obligations, the Big Five went from 35% in FY 2017 to 32% in FY 2018. In total over the course of the defense contacting rebound, defense contract obligations awarded to the Big Five increased 32% from FY 2015 to FY 2018.

Large vendors initially fared the worst during the initial two years of the rebound, declining 1% between FY 2015 and FY 2017, but experienced their own rebound in FY 2018. Defense contract obligations awarded to Large vendors totaled $102.4 billion in FY 2018, a 14% increase from FY 2017's $89.9 billion. However, Large vendors have yet to recover as a share of total defense contract obligations, accounting for only 28% of total defense contract obligations in FY 2018 as opposed to their 31% market share in FY 2015.

Small and Medium vendors both continued to benefit from the defense contracting rebound. In FY 2018, defense contract obligations awarded to Small and Medium vendors increased 16% and 18%, respectively. Between FY 2017 and FY 2018, the share of total defense contract obligations awarded to Medium size vendors rose from 19% to 21%, while Small vendors rose from 19% to 20%.

Figure 7 shows defense contract obligations by vendor size from FY 2000 to FY 2018.

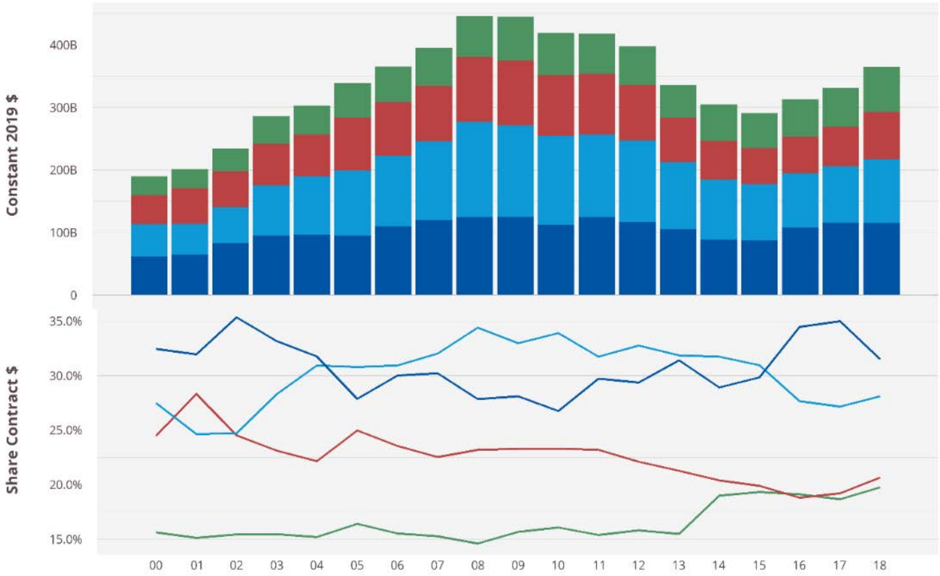


Figure 7. **Defense Contract Obligations by Vendor Size, 2000–2018**
(Source: FPDS; CSIS analysis)

[1] The Big Five are the five largest defense contractors as measured by total defense contract obligations: Lockheed Martin, Boeing, Northrup Grumman, Raytheon, and General Dynamics.

Vendor Count

Previous CSIS research showed that both the total number of prime vendors doing business with the DoD and the number of new prime entrants to the defense market had been declining in recent years (McCormick et al., 2017; Cohen et al., 2018). As shown in Figure 8, both of these trends continued in FY 2018. The data show that in FY 2018, the number of total prime vendors doing business with the DoD declined 9%, while the number of new prime vendors declined 7%. Since FY 2015, the total number of prime vendors doing business with the DoD has fallen 15%, while the number of new prime vendors has declined 16%. These trends, particularly the continued decline in the number of new entrants, is troublesome as the DoD emphasizes the National Security Innovation Base and tries to attract non-traditional defense companies to do business with the DoD.

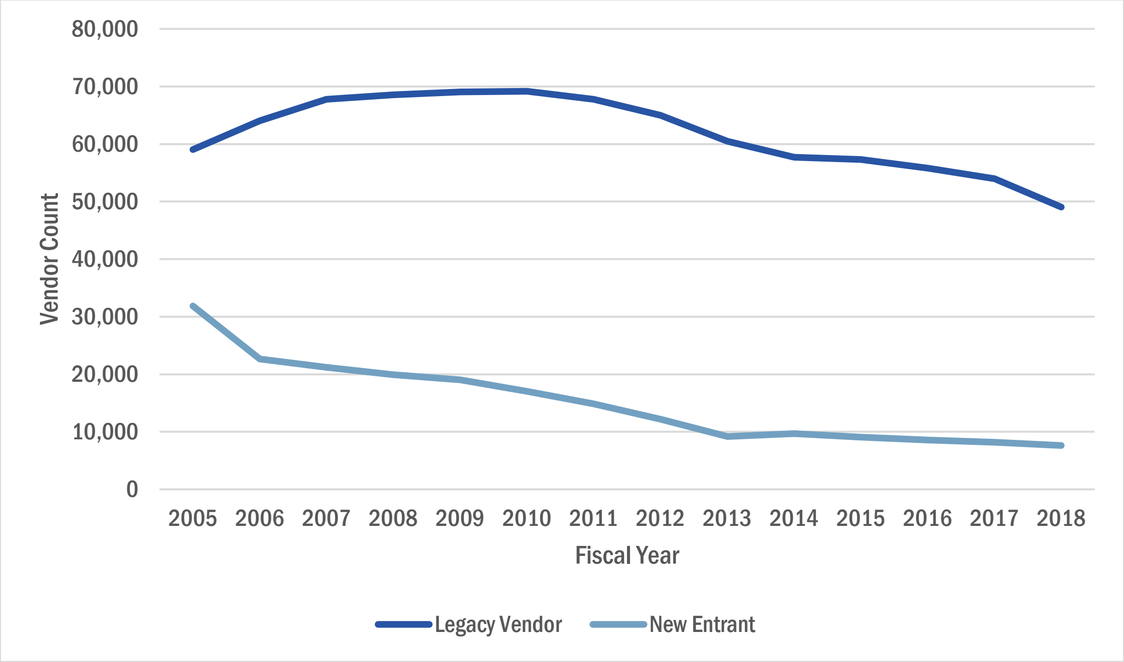


Figure 8. **DoD Vendor Count, 2005–2018**
(Source: FPDS; CSIS analysis)

Defense Components

Navy contract obligations grew 25% between FY 2015 and FY 2017, the most of any component, but fell in FY 2018. Navy contract obligations decreased from $113.1 billion in FY 2017 to $109.7 billion in FY 2018, a 3% decline. As a share of total defense contract obligations, the Navy fell from 34% to 30%, a market share more in line with historical averages.

The Air Force continued its year-to-year whipsaw in FY 2017, as Air Force contract obligations increased 15% last year. Air Force contract obligations are up 30% from FY 2015, but the year-to-year data shows the volatility of Air Force contracting trends in recent years. Over the last four years, Air Force contract obligations have gone from $56.2 billion in FY 2015 to $68.4 billion in FY 2016 before declining to $63.1 billion in FY 2017 and then increasing again in FY 2018 to $72.8 billion.

The Army had been growing at a slow but steady rate over the last two years after being the large bill-payer during sequestration and the defense drawdown, and saw a large upswing in FY 2018 (McCormick et al., 2018). Army contract obligations increased 15% in FY 2018, going from $80.97 billion to $93.17 billion.

Both the Defense Logistics Agency (DLA) and the Missile Defense Agency (MDA) grew at rates significantly above the defense topline in FY 2018. In FY 2018, DLA and MDA contracting obligations reached near-historic levels, increasing 26% and 51%, respectively.

Figure 9 shows defense contract obligations by component from FY 2000 to FY 2018.

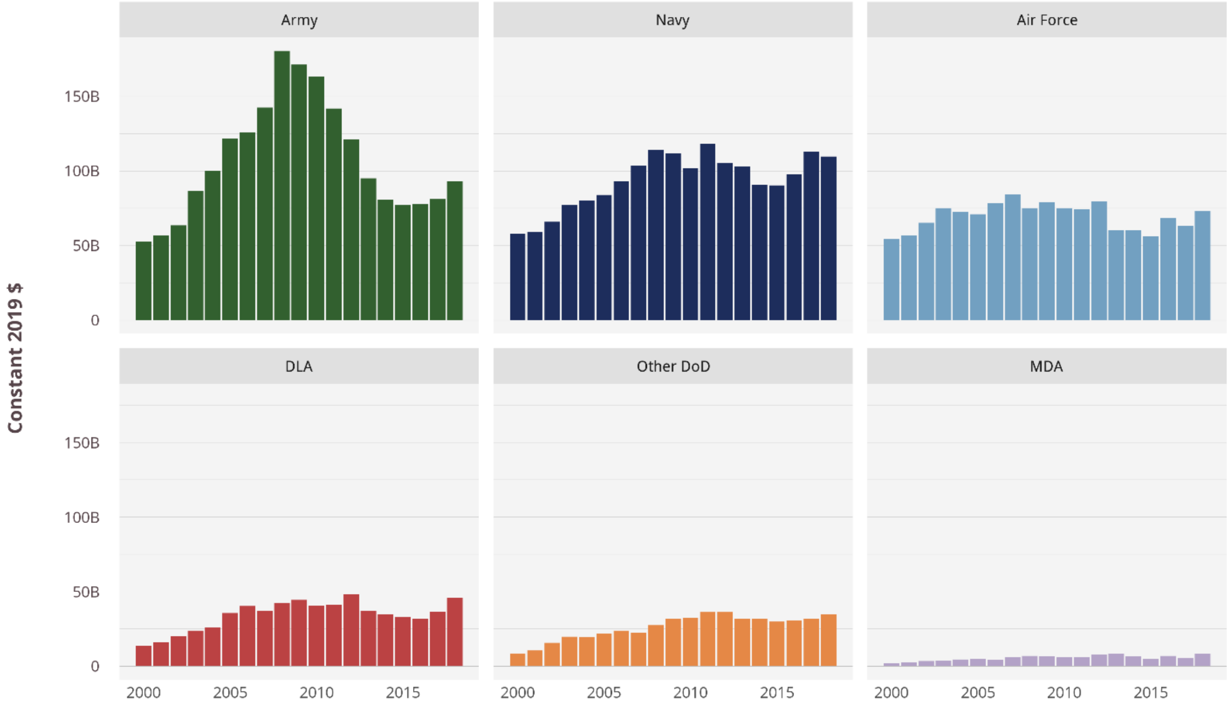


Figure 9. **Defense Contract Obligations by Component, 2000–2018**
(Source: FPDS; CSIS analysis)

Conclusion

No significant shift in the DoD's investment between products and R&D to reflect modernization priorities emphasized in 2018 National Defense Strategy

There was not a significant shift in the DoD's FY 2018 investment between products, services, and R&D despite the 2018 National Defense Strategy emphasizing modernization and the importance of great power competition. Although DoD spending on defense services caught up to spending on products in FY 2018, R&D contract obligations continue to trail far behind the other two areas of the DoD's investment portfolio. At the same time that the DoD is emphasizing the importance of modernization to meet the 2018 National Defense Strategies' priorities, in FY 2018, R&D fell to the lowest it has ever been this century as a share of total defense contract obligations.

Aircraft down; Land Vehicles and Facilities and Construction bounce back; Air & Missile Defense, and Ordnance & Missiles up

While there have not been significant shifts in the DoD's investment between products, services, and R&D, there were more significant changes at the sector level in FY 2018.

Land Vehicles and Facilities and Construction, two of the sectors hardest hit by sequestration and the defense drawdown, rebounded rather significantly in FY 2018. Land Vehicles contract obligations increased 51% in FY 2018, rising from $8.5 billion in FY 2017 to $12.9 billion in FY 2018, the highest level of Land Vehicles spending in the last six years. Facilities and Construction defense contract obligations increased 20% in FY 2018, twice the overall rate of growth.

Aircraft contract obligations, which had been the biggest beneficiaries of the first two years of the defense contracting rebound, declined 5% in FY 2018. This decline isn't too surprising as the Aircraft sector has been previously shown to be vulnerable to whipsawing back and forth between growth and declines.

Other notable trends include the year-to-year whipsaw in the Air & Missile Defense sector and steady growth in Ordnance & Missiles spending. While Air & Missile Defense contract obligations increased 37% from FY 2015 to FY 2018, a rate well above the 25% growth in total defense contract obligations, there has been a significant whipsaw year-to-year. After Air & Missile Defense contract obligations declined 15% in FY 2017, contract obligations subsequently increased 53% in FY 2018. Comparatively, Ordnance & Missiles contract spending increased 56% from FY 2015 to FY 2018, but with consistent growth year-to-year. In FY 2018, Ordnance & Missiles obligations increased 51%, and spending last year totaled levels not seen since FY 2007 to FY 2009.

Uneven recovery from the trough in the development pipeline for major weapon systems

The data show that the DoD has made some recovery in its development pipeline for major weapon systems, but recovery has been uneven across the different R&D activities. Despite System Development & Demonstration contract obligations increasing in FY 2017 for the first time since FY 2005, they subsequently declined 6% in FY 2018. In FY 2018, System Development & Demonstration contract obligations accounted for just 15% of total defense R&D contract obligations, whereas they have historically accounted for approximately 27% of annual defense contract obligations.

The largest recovery came in the mid-stage of the weapon systems pipeline where Advanced Technology Development (6.3) and Advanced Component Development & Prototypes (6.4) grew at rates well above the overall growth in defense R&D contracts in FY 2018. Of note, as the DoD has been emphasizing increasing experimentation and prototyping in the acquisition process, Advanced Component Development & Prototypes accounted for 23% of total defense R&D contract obligations in FY 2018, well above the historical average of 14% (McCormick et al., 2019).

OTA usage continues increasing across DoD

OTAs continue to gain popularity across the DoD following the recent legislative changes aimed at incentivizing their usage. Total OTA obligations across the DoD increased 81% in FY 2018 from FY 2017. Over the last three years, total DoD OTA obligations have increased 352% from FY 2015.

The data also show that total potential value of OTA agreements signed in recent years is growing at over twice the rate of OTA obligations. Between FY 2015 and FY 2018, the total potential value of OTA agreements, were they to exercise all of their options, increased 352%.

The Army remains the predominant user of OTAs across the DoD, in large part due to its OTA Center of Excellence located at Picatinny Arsenal, but the other components have substantially increased their usage of OTAs in the last year. Army OTA obligations increased 86% last year and are up 348% from FY 2015. The Air Force made some limited use of OTAs prior to the recent legislative changes but has seen a 9982% increase in Air Force OTA obligations since FY 2015. Finally, the Navy has historically made little use of OTAs, accounting for less than 1% of all defense OTA obligations prior to FY 2018. While the Navy did make significantly greater usage of OTAs in FY 2018 than it had previously, it still only accounted for 1% of FY 2018 defense OTA obligations.

Big Five decline in FY 2018; Growth relatively evenly between Small, Medium, and Large

The Big Five benefited the most from the first two years of the defense contracting rebound but declined 1% in FY 2018. Instead, the 10% increase in total defense contract obligations in FY 2018 was relatively evenly distributed between Large, Medium, and Small vendors. Of note, Small vendors accounted for 20% of total defense contract obligations in FY 2018, their highest share of total defense contract obligations this century.

Number of prime vendors and new entrants doing business with DoD continues to decline

The data show that the number of prime vendors and new entrants doing business with the DoD continued declining in FY 2018. In FY 2018, the number of prime vendors doing business with the DoD declined 9%, while the number of new prime entrants declined 7%. Although defense contract obligations have increased 25% since FY 2015, the number of prime vendors doing business with the DoD has fallen 15%, while the number of new prime entrants has fallen 16%. Given the importance the DoD has placed on attracting new entrants, particularly non-traditional defense companies, these trends are worrisome.

Air Force bounces back; Navy starts decline; Army sees large upswing; MDA and DLA hit near-historic levels

There were notable differences in the contracting trends between the military components during the first two years of the defense contracting rebound and the FY 2018 trends.

Air Force contract obligations bounced back in FY 2018, increasing 15% from FY 2017. This continued the Air Force's year-to-year whipsaw between total contract obligations growing one year and declining the next, a trend that has been ongoing since FY 2015.

The Navy benefited the most during the first two years of the defense contracting rebound, hitting historic levels this century as a share of total defense contract obligations, but returned to more historic levels in FY 2018, experiencing a 3% decline in contract spending from FY 2017.

Army contract obligations, which had been growing at a slow but steady rate over the last two years after being the heaviest hit during sequestration and the defense drawdown, increased 15% in FY 2018.

Finally, DLA and MDA contract obligations increased 26% and 51%, respectively, in FY 2018 as these components' contract spending totaled near historic levels for this century.

Final Thoughts

The FY 2018 defense contracting data provides critical insights into the defense acquisition system's response to the 2018 National Defense Strategy and new administration's priorities. While the new administration had the opportunity to influence some of the trends seen in the FY 2017 defense contracting data, FY 2018 represents the first fiscal year fully executed by this administration.

Overall, the defense acquisition system has had a mixed response to the 2018 National Defense Strategy and the new administration's priorities. While you can look at most of the contract characteristics analyzed in this paper and see reflections of the National Defense Strategy and administration priorities, the interconnective thread that sews together the disparate data points is seemingly missing. For example, you look at the platform portfolio contracting trends and see increased investment in Air & Missile Defense in FY 2018, but this is not reinforced by any significant shifts in the composition of the DoD's investment portfolio between products and R&D. You look at the weapon systems pipeline trends and see Advanced Component Development & Prototypes (6.4) contract obligations at historic levels in FY 2018, as a share of total defense R&D contract obligations, but also a return to declining System Development & Demonstration (6.5) contract obligations.

If the DoD is to succeed at refocusing itself on peer and near-peer competition and forging a new relationship between the DoD and the National Security Innovation Base, and better recognize that interconnective threads are missing from the emerging from the FY 2018 defense contracting trends and explore why that is. How does the DoD balance its investment portfolio while also maintaining readiness through procuring and maintain existing platforms and fielding new modernization programs in the near-term despite continued cuts to System Development & Demonstration (6.5) while also leaving room for longer-term modernization funding? Why has the DoD continued to struggle to attract new entrants in recent years despite defense contract spending increasing 25% the last three years and several policies aimed at attracting new vendors, to include non-traditional defense companies? Understanding and addressing these missing interconnective threads are an evergreen issue for every administration but are of critical importance given that decisions today could transform the defense acquisition system and supporting industrial base for the next 10 to 20 years.

This paper presents only the initial findings of CSIS's analysis of the FY 2018 defense contracting trends in the FPDS. CSIS will continue to refine and expand its analysis on the trends presented in this paper and more in future reports.

References

Cohen, S., Sanders, G., Mooney, S., & Roth, M. (2018). *New entrants and small business graduation in the market for federal contracts*. Washington, DC: Center for Strategic and International Studies. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181120_NewEntrantsandSmallBusiness_WEB.pdf.

DoD. (2018). *Summary of the 2018 national defense strategy of the United States of America: Sharpening the American military's competitive edge*. Retrieved from https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

McCormick, R., Cohen, S., Sanders, G., & Hunter, A. P. (2019). *Defense acquisition trends, 2018: Defense contract spending bounces back*. Washington, DC: Center for Strategic and International Studies.

McCormick, R., Cohen, S., Sanders, G., Hunter, A. P., Huitink, Z., Mooney, S., & Roth, M. (2018). *Trends in industry: Key findings and insights from 2018 CSIS research*. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181130_DIIG_ExecutiveSummaryAnthology_WEB_update.pdf

McCormick, R., Hunter, A. P., & Sanders, G. (2017). *Measuring the impact of sequestration and the drawdown on the defense industrial base*. Washington, DC: Center for Strategic and International Studies. Retrieved from https://www.csis.org/analysis/measuring-impact-sequestration-and-drawdown-defense-industrial-base

McCormick, R., Hunter, A. P., Sanders, G., Cohen, S., & McQuade, M. R. (2015). *Measuring the outcomes of acquisition reform by major DoD component*. Washington, DC: Center for Strategic and International Studies. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150930_McCormick_MeasuringOutcomesAcquistionReform_Web.pdf

Disclaimer

The Center for Strategic and International Studies (CSIS) does not take specific policy positions; accordingly, all views expressed in this presentation should be understood to be solely those of the author(s).

Panel 2. Cybersecurity Acquisition—Software and Risk Implications

Wednesday, May 8, 2019	
10:30 a.m. – 11:45 a.m.	**Chair: Captain Melvin Yokoyama, USN,** Commanding Officer, Naval Information Warfare Center (NIWC) Pacific **Discussant: Howard Pace,** Professor of the Practice, Naval Postgraduate School ***Acquisition of Software-Defined Hardware-Based Adaptable Systems*** Maura McQuade and Andrew Hunter, Center for Strategic and International Studies ***Acquisition System Design Analysis for Improved Cyber Security Performance*** Brad Naegle, Naval Postgraduate School

Captain Melvin Yokoyama, USN—A native of the Big Island of Hawaii, Captain Yokoyama holds a Bachelor of Science degree from Jacksonville University and a Master of Science degree in Systems Engineering (Information Warfare and Electrical Systems Engineering subspecialties) from the Naval Postgraduate School.

A designated Naval Flight Officer in the Unrestricted Line (URL) community, Capt. Yokoyama is a member of the Defense Acquisition Corps and a Level II Joint-qualified Officer.

At-sea assignments include duties as commanding officer and executive officer of Tactical Air Control Squadron TWELVE (TACRON 12), Air Officer for the Bonhomme Richard Amphibious Ready Group, Officer-of-the-Deck (underway) for the USS Ronald Reagan (CVN-76), officer-in-charge commander Task Group 57.1 (Manama, Bahrain and Al Udeid, Qatar), officer-in-charge commander Task Group 72.5 (Misawa and Okinawa, Japan), EP3E operations officer for Fleet Air Reconnaissance Squadron ONE (VQ-1), and ES-3A electronic warfare mission commander for Fleet Air Reconnaissance Squadron SIX (VQ-6) deployed onboard the USS Enterprise (CVN-65) and USS John F. Kennedy (CV-67).

Acquisition and shore assignments include duties as principal assistant program manager (PAPM) at PEO C4I Information Assurance and Cyber Security Program Office (PMW-130), assistant program manager (APM) for SPAWAR's Data Center and Application Optimization (DCAO) program office, chief of staff for the Department of the Navy's Data Center Consolidation Task Force, deputy commander and Tomahawk Land Attack Missile (TLAM) C4I officer for U.S. Strategic Command's (USSTRATCOM) Cruise Missile Support Activity Pacific, and as a graduate student in the Information Warfare curriculum at the Naval Postgraduate School.

Capt. Yokoyama recently returned from a one-year global war on terrorism (GWOT) individual augmentation (IA) assignment to the U.S. Embassy, Baghdad, Iraq where he served as the senior military advisor to the Iraqi Minister of Defense in support of Operation INHERENT RESOLVE.

Capt.Yokoyama's personal awards include the Legion of Merit, Defense Meritorious Service Medal (two awards), Meritorious Service Medal (two awards), Air Medal (individual award), the Navy Marine Corps Commendation Medal (three awards), the Navy Marine Corps Achievement Medal (three awards), and various unit awards and campaign medals.

Howard Pace—Mr. Pace serves as Professor of the Practice at the Naval Postgraduate School, Graduate School of Business and Public Policy. His teaching and research interest are in acquisition, program management and acquisition reform. He is also a sole proprietor of Pace Enterprises where Mr. Pace consults on space, cyber and RF networking technologies, acquisition and strategies. Before joining NPS, Mr. Pace served in several Industry positions as Vice President. He was responsible for creating, communicating, planning and executing strategic initiatives and business development opportunities.

Mr. Pace enlisted in the Navy, rising to the rank of Chief Petty Officer while serving in the Submarine Force. He graduated from the University of Washington with a degree in Mechanical Engineering where he received his commission. He qualified as a Surface Warfare Officer in USS ELROD (FFG-55) and served during Operation Desert Storm, Southern Watch, Joint Endeavor, and Support Democracy. He also served aboard USS SAN JACINTO (CG-55) and USS GEORGE WASHINGTON. Mr. Pace was selected as an Engineering Duty Officer, Acquisition Professional and graduated from NPS with a Master's degree in Electrical Engineering. He spent his subsequent assignments at the Space and Naval Warfare Systems Command (SPAWAR) in San Diego, CA serving as the Chief Engineer of Naval Communications. Mr. Pace retired from the U.S. Navy and began his career as a civil servant, serving as Technical Director of PEO C4I and Space and as the Navy's IA Certification Authority for all Naval C4ISR systems. Mr. Pace began his joint service as the Deputy Joint Program Executive Officer (DJPEO), Joint Tactical Radio System (JTRS) and was selected as a Member of the Senior Executive Service. Mr. Pace assumed the role of Joint Program Executive Officer and was responsible for the acquisition, operational testing and initial deployment of JTRS across joint forces.

Acquisition of Software-Defined Hardware-Based Adaptable Systems

Maura Rose McQuade—was a program manager and research associate in the Defense-Industrial Initiatives Group at CSIS from 2017 to 2019. [mrm310@georgetown.edu]

Andrew Hunter—is a senior fellow in the International Security Program and director of the Defense-Industrial Initiatives Group at CSIS. From 2011 to 2014, he served as a senior executive in the Department of Defense, serving first as chief of staff to Under Secretaries of Defense (AT&L) Ashton B. Carter and Frank Kendall, before directing the Joint Rapid Acquisition Cell. From 2005 to 2011, Hunter served as a professional staff member of the House Armed Services Committee. Hunter holds an MA degree in applied economics from the Johns Hopkins University and a BA in social studies from Harvard University. [ahunter@csis.org]

Schuyler Moore—was a research intern in the Defense Industrial Initiatives Group at CSIS in 2018. [schuyler.c.moore@gmail.com]

Abstract

The increasing importance of software has created an opportunity for the Department of Defense (DoD) to harness innovation through the acquisition and modification of systems that are (1) inherently multifunctional and (2) designed for continuous modification. Examples of these types of systems include radars, electronic warfare pods, and electro-optical sensor suites and are referred to here as adaptable systems. Identifying an acquisition approach to these types of adaptable systems that are software-defined and hardware-intensive is particularly challenging from an acquisition perspective. The optimal timeline for these systems does not fall into typical acquisition phases that discretely differentiate between phases such as research and development and production. The study team at CSIS has examined how the DoD presently acquires these systems and identified potential solutions to overcome the barriers found when adopting adaptable systems, some of which include more agile acquisition processes, open systems architecture, DevOps, flexible funding, development sprints, increased user feedback, and prototyping.

Introduction

Today's security environment requires the United States to prepare for defense against a wide range of adversaries. The 2018 National Defense Strategy (NDS) emphasizes that both the prosperity and security of our country is challenged by the reemergence of long-term strategic competition, a resilient but weakening post-WWII international order, and rogue regimes and non-state actors that destabilize regions critical to international security (DoD, 2018). Each of these adversaries is adopting and deploying technology in new and innovative ways, challenging the United States to be able to rapidly respond and adapt to a variety of threats. The Department of Defense (DoD) must reexamine almost every facet of its operations to assess what changes are required to enable effective responses to these new threats, and as part of this effort, the acquisition system is rightly considered a central element requiring reform.

Reform of the acquisition system is a continuous process undertaken by both the DoD and Congress in pursuit of objectives that are sometimes, but not always, aligned. In light of the 2018 NDS, the impetus for acquisition reform has shifted for both the DoD and Congress from a previous priority on cost control to a new emphasis on speed. This shift, while necessary in many respects, is not sufficient to address the requirements of the NDS. In addressing the need for greater speed, great attention has been given to streamlining, accelerating, and reforming how the acquisition process works. Comparatively less attention, however, has been given to the question of what the process is being optimized to deliver. This problem is critical because systems capable of responding to the wide range of changing threats identified in the NDS—adaptable systems—face a number of barriers in the current acquisition system. This paper identifies the need for and characteristics of adaptable systems, the barriers they face in the current acquisition system, the enablers that can allow for their successful development and deployment, and potential changes for the acquisition system that result from this analysis.

Section 1: The Need for Adaptable Systems

As the NDS notes, today's security environment is increasingly complex and defined by rapid technological advancement and changing character of war, where "the drive to develop new technologies is relentless, expanding to more actors with lower barriers to entry, and moving at accelerating speeds" (DoD, 2018). This rate of change challenges the United States to meet a variety of different threats, which are advancing and changing by the day. It states, "Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting" (DoD, 2018). The future threat environment suggests technological superiority or inferiority will not be static; instead, with the rise of peer competitors, defending national security necessitates the ability to quickly and flexibly leverage areas of strength and mitigate areas of weakness. History demonstrates that technological superiority may not always win wars; however, refusal to adapt to changing technology will almost always lose wars. Future success is therefore dependent on the nation's ability to adapt and rapidly adjust to uncertainties in threats, nimble adversaries, rapidly emerging (and obsolescence of) technologies, and new domains.

The rapid technological change occurring in commercial technology is a key driver in the strategic environment. Commercial technology development methods have advanced toward more agile processes that are better able to meet a rapidly evolving set of user-needs and customer demands. This shift is especially true in the area of software. Commercial industry is deploying continuous, iterative software-development that can harness technology advances, merge previously separate functions, continuously upgrade, utilize machine learning, and better leverage user feedback. The ability to use rapid developing commercial technology to drive adaptability in military operations is as equally available to potential U.S. adversaries as it is to United States and its as allies.

What Adaptable Systems Can Bring to Defense

The U.S DoD can capitalize on technology trends that have developed to meet rapidly evolving user-needs and customer demands through the design of adaptable systems. Adaptable systems are systems that have the inherent ability to deliver a wide variety of capabilities from a single basic design (multifunctionality) and can readily add capability over time (growth) at what former Defense Secretary Jim Mattis would term "the speed of relevance."

Adaptable systems are not new. Traditionally, features such as multifunctionality and growth potential were delivered in defense by very expensive, high-end systems that designed in excess space, weight, and power to support the addition of additional sensors and weapons. The classic example of this traditional approach to adaptable systems in defense are Navy ships, which grew ever larger in the 20th century to support a wide variety of missions and address a wide range of threats. In the 20th century, adaptability was an aspect of the most expensive systems in the arsenal and was a major cost driver.

The commercial technology sector has embraced a different approach to adaptable systems, using continuous, iterative software-development that can harness technology advances, merge previously separate functions, continuously upgrade features, utilize machine learning, and better leverage user feedback. The classic commercial sector example of an adaptable system is the smartphone, which has developed to absorb the functions of many previously separate devices, almost entirely through added software and networking. Increasingly, however, it is becoming clear that the characteristics of adaptable systems can also be achieved more cheaply and more successfully in the defense sector through writing new software rather than building and adding new hardware.

Today's systems don't require massive scale and expense to achieve adaptability. Increasingly, they achieve adaptability because the most important elements of functionality are defined in software and can be modified without substantial changes to the hardware. As a result, a piece of gear that can transmit and receive electrons may be a radio, radar, and an EW asset simultaneously, and it can be upgraded quickly as the technology evolves. These systems are hardware-based, but software-defined.

Additional Advantages of Adaptable Systems

While there is a compelling rationale for developing adaptable systems to compete with adversaries who are likely to be attempting to do the same, there are additional, inherent benefits to the use of adaptable systems. Adaptable systems, because they are designed to readily add additional capability, can speed the deployment of the key new technologies identified in the NDS, such as artificial intelligence and directed energy. Deploying these technologies in support of military missions requires integrating them in some form into new or existing military platforms, which adaptable systems can support. Adaptable systems can also reduce risk. The iterative, evolving nature of adaptable systems means that individual modifications are continuous and highly incremental. This creates the opportunity to reduce the scope of risk included in any individual upgrade as well as the ability to fail fast and move on when necessary.

While adaptable systems will present challenges to industry, particularly prime contractors who will have to manage in a far more dynamic environment, they also bring benefits to industry at multiple tiers of the supply chain. At the level of subsystem suppliers and component developers, adaptable systems create the opportunity for enhanced competition as the frequent modification and upgrade cycles generate new market opportunities on a regular basis. While electronics obsolescence is always a challenge, adaptable systems may be able to effectively avoid and mitigate technology obsolescence in subsystems and components more effectively, extending the useful service life of adaptable systems. Similarly, adaptable systems can ease the process of adapting U.S.-built systems for allied needs and/or incorporating interoperability with U.S. systems into allied equipment. In terms of life cycle costs, individual adaptable systems may not be cheaper to own than systems that hew closer to a static baseline, but it is possible that the efficiency of adaptable systems spending, in terms of capability delivered per dollar expended, could be high. Such increased efficiency in the DoD's acquisition spend could translate into savings elsewhere in the overall defense budget.

The Challenges of Adaptable Systems

Adaptable systems are inherently hybrid in nature. Because they are hardware-based, that is, they often have a metal superstructure such as on the array on a radar system, they look like hardware systems to the acquisition system and are generally handled as such. Because they are software-defined, however, it is the 1s and 0s of code that truly generate the bulk of the military capability that they deliver. However, acquisition processes developed solely for software may not address important aspects of what the and adaptable system is required to do. Adaptable systems still need to develop their sophisticated hardware elements as well as their software elements. An acquisition system that can successfully leverage the software components of hardware-based systems will harness continuous development, multi-functionality, and adaptability.

The multifunctionality of adaptable systems also can present challenges due to the interdependent nature of these functionalities. The Defense Science Board notes that "Unexpected complications can arise from unanticipated interdependencies within the software itself, often driven by the underlying architecture. A current DoD acquisition best practice is to reduce project risk by specifying the function of the software in detail at the beginning of a program" (Defense Science Board, 2017, p. 7). The more multifunctional and adaptable a system is, the more challenging it is to forecast the scope of its functionality and predict the independencies from the start.

Section 2: Adaptable Systems Usage in Defense

Before further discussing the barriers and enablers associated with developing and deploying adaptable systems for military missions, it is useful to examine some examples of the usage of adaptable systems in defense in greater detail.

Battlefield Airborne Communications Node

An example of adaptable systems in defense is the Air Force's Battlefield Airborne Communications Node (BACN), which originally leveraged a commercial aircraft base, relatively simple networking nodes, and lots of software to serve as a critical theater network hub connecting disparate parts of the joint force (Hlad, 2017). Since its initial development, the BACN capability has also been incorporate on unmanned platforms such as the Global Hawk. BACN is the opposite of the exquisite, expensive multi-functional military platforms of previous decades. It leverages the inherent ability of software-defined systems to deliver multifunctionality and growth by adding new code rather than new hardware incorporating additional communications links that allow it to connect more systems together as needed over time.

BACN provides a communications relay by translating data links and voice systems into a common output. This data sharing contributes to three objectives: it improves interoperability of platforms and systems using disparate communication forms, it allows ground troops to "see" the battlespace beyond the horizon, and it provides improved situational awareness and a common battle picture for all parties in a joint operation. BACN was initially developed as a Quick Reaction Capability (QRC) to address a Joint Urgent Operational Need (JUON) and was named a Program of Record in 2018. The system was originally meant to be a technology demonstration, but the Air Force was able to accelerate BACN development and fielded the system ultimately delivering four integrated BACN systems within 16 months (Northrop Grumman, n.d.).

Surface Electronic Warfare Improvement Program

The Surface Electronic Warfare Improvement Program (SEWIP) is an electronic warfare system comprised of radar warning receivers and active jamming systems and is integrated with a ship's self-defense system to trigger the deployment of decoys and flares in the event of an attack (Defense Industry Daily, 2019). SEWIP supports early detection, analysis, threat warning, and protection from anti-ship missiles.

The program uses an "evolutionary acquisition and incremental development" strategy to upgrade each system (U.S. Navy, 2017). SEWIP is modular with open architecture and is upgraded in blocks; SEWIP Block I was focused on obsolescence mitigation and special signal intercept, Block II provided electronic support capability improvement, Block III is in the process of adding electronic attack capabilities, and Block IV will integrate EO/IR capabilities onto the existing electronic warfare system (LaGrone, 2015). The most recent upgrade to Block III includes a shift to solid-state digital receivers and transmitters, allowing for more reliability and easier maintenance while making the system more adaptable (Freedberg, 2016). SEWIP exemplifies the multifunctionality available in an adaptable system by using primarily software changes to allow it to perform electronic warfare, electronic attack, and electronic intelligence functions.

AEGIS

The Aegis Weapon System is one of the more high-profile examples of a system shifting from a closed, hardware-dependent structure to an open, software-dependent one. Aegis was first fielded on a commissioned U.S. Navy ship in 1983, and the Navy's fleet of Ticonderoga-class cruisers and Arleigh Burke-class destroyers have all been outfitted with Aegis. The newest 11 cruisers and the whole fleet of destroyers are undergoing modernization that converts Aegis into an open architecture format, in addition to various HM&E upgrades (U.S. Navy, 2019). Additionally, the USS *Arleigh Burke* will be the first destroyer to be modernized to merge Aegis open architecture with Aegis BMD with the goal of ultimately giving the entire destroyer fleet BMD capabilities (Pearn, 2008).

The business model for Aegis' open architecture transition is composed of four parts. First, it requires concurrent development, integration, and testing to upgrade software capabilities. Second, it applies modern software engineering processes with agile development, rather than the traditional waterfall development. Third, it opens competition up to multiple commercial vendors for individual components of the software. Finally, it leverages points of overlap in capability development across weapons systems (DeLuca et al., 2013).

This process has taken place over multiple decades and ship upgrades. The first step was to implement COTS infrastructure and systems onto cruisers and destroyers to simplify the upgrade process and set a common standard. Next, some systems were broken down into component-based software decoupled from hardware to allow for a layered architecture and spiral development (software upgrades can now occur every two years while hardware refreshes occur every four). In recent years, more systems within Aegis have been transitioned to this open architecture framework based on their common set of components and application programming interfaces, referred to as "Baseline 9" (Durbin & Scharadin, 2011). As a result of the evolution of Aegis, it now functions as an adaptable system.

The current Aegis modernization program builds on previous upgrades and software developments. The next phases of development will include Aegis Modernization (AMOD) Advanced Capability Build 12 for both destroyers and cruisers, with each phase focused transitioning more components of Aegis to open architecture and allowing increased data sharing and communication between Aegis ships and the rest of the fleet.

Joint Tactical Radio System

An example of a program that experienced major challenges in part because it struggled to develop the characteristics of an adaptable system is the Joint Tactical Radio System (JTRS). The JTRS program (the JTRS program office was disbanded in 2012) sought to develop a set of software-defined radios intended to replace all existing radios in the U.S. military. JTRS sought to enable communication across a range of frequencies and waveforms, allowing increased interoperability both within the U.S. military and with U.S.

allies by converting analogue signals to digital. The JTRS program was built around the Software Communications Architecture (SCA) as an open architecture framework to enable rapid, flexible upgrades, and all JTRS components had to be SCA compliant (Military and Aerospace Electronics, 2004). The system comes in various formats: Network Enterprise Domain (NED); Ground Mobile Radios (GMR, now cancelled); Handheld, Manpack & Small Form Fit (HMS); Multifunctional Information Distribution System (MIDS); and Airborne & Maritime/Fixed Station (AMF). All systems can be upgraded with new software via a wireless information network, allowing for rapid insertion of new technologies across a broad range of systems.

However, the JTRS program has faced significant challenges along the way. Although GMR was certified for use in 2012, the Army ultimately cancelled that branch of the program due to cost overruns and technical challenges the program faced along the way. When the program first started, SDR technology was in its infancy, but JTRS GMR tried to accomplish too much and was constantly shifting hardware design and software requirements throughout the development phase. Furthermore, JTRS failed to adopt an agile approach that would have allowed for user feedback throughout the development process—instead, the program adopted a waterfall methodology that only allowed users to interact with the system after 13 years of development, by which point the problems in GMR were solidified and difficult to reverse (Gallagher, 2012). At the same time, developments in commercial SDR led industry to develop radios outside the JTRS program that provided capabilities the JTRS program had not been able to deliver. As a result, the JTRS GMR program was terminated in 2011.

Some programmatic descendants of the JTRS program are continuing to move forward. MIDS/JTRS has been successfully integrated onto platforms both in the United States and sold overseas, allowing for increased data interoperability between NATO countries. Both JTRS HMS and AMF has been fielded at low-rate initial production and its variants continue to be tested (Gallagher, 2018).

Section 3: Barriers to Adaptable Systems

While the case for the use of adaptable systems in defense is strong and there is a history of developing such systems in certain instances, there are reasons why such systems are not widespread. There are substantial barriers to the development and deployment of adaptable systems inherent in the defense acquisition system. It is crucial to understand what these barriers are and how they operate in order to develop an approach to overcoming them.

Design of the Traditional Acquisition System

For the DoD, adaptable systems are essential to fully leverage the capabilities of existing technologies to meet future warfighting needs. Software-defined, adaptable systems will play an increasingly critical role going forward. But these types of systems test the limits of the current acquisition system, which is accustomed to acquiring systems in a much more tightly defined and linear manner. As a result, the DoD has struggled to evolve at the same pace as commercial technology. The defense acquisition system was originally focused on Major Defense Acquisition Programs (MDAP) with long development cycles, enormous quantities, and tightly defined requirements because the system was designed to provide oversight to high-value hardware systems that were planned to remain in production for decades.

MDAPs almost always begin with highly detailed, highly defined requirements that specify in advance what threats a system is likely to confront and how it is expected to operate in military missions. While useful, this approach introduces the risk of over specifying systems toward problems which may morph rapidly over the long development and delivery time scales of defense acquisition.

The DoD 5000.02 acquisition milestone process is designed to progressively reduce technical risk by proceeding through discreet phases of development, test, and evaluation before entering full-rate production (DoD, 2015). If upgrade increments are planned, they are usually executed serially, not simultaneously. There are high transaction costs for change and high thresholds for justifying a new increment. Communication between the different elements of the acquisition system are organized around acquisition milestones and toward executing Milestone Decision Authority (MDA) directives. Such events are rare, and the stakes are high because the system is loath to deviate from or reverse these decisions.

However, adaptable systems (like other software-oriented development efforts) work best when developed in conjunction with frequent iterative feedback loops throughout the process. Under an adaptable systems approach, acquisition programs would be engaged simultaneously in development, production, and sustainment, which are not easily disentangled for review according to the traditional milestones. Instead, adaptable systems require continuous communication on requirements, budgets, and acquisition benchmarks.

Traditional acquisition metrics can be a major problem for adaptable systems. The Earned Value Management System (EVMS) is a common tool for measuring progress in acquisition programs. It is designed around breaking down a program’s master schedule throughout its entire development into discrete work packages that register as earned value when they are completed at or below expected costs. EVMS as traditionally implemented, however, requires an almost entirely static program baseline, to function. When the content of work packages is subject to continuous change, the ability of EVMS to meaningfully track progress on the program decays rapidly. Given this contrast between the DoD 5000.02 acquisition system’s need for discreet acquisition phases and benchmarks and adaptable systems’ more fluid development processes, the traditional approach to acquisition hinders the critical elements for success for an adaptable system.

Budgeting

Current acquisition budgeting also presents roadblocks for adaptable system given the defense acquisition system orientation around MDAPs. Budgets for acquisition programs provide prescriptive funding at levels set years in advance that may be incompatible with the rapidly evolving needs of an adaptable system. Adaptable systems consider multiple new and expanded features for the upgrade cycle simultaneously. They will struggle in a budget process that requires both projections five years into the future for every technology insertion and detailed production and sustainment plans before moving forward on allocating development resources. There is precious little evidence of success in technology development that is budgeted outside of an MDAP and then transitioning into a major system, something that would have to happen frequently for adaptable systems to realize their true promise.

The DoD’s budgeting process also includes separate “colors of money” for research and development, production, and operation and maintenance designed to support systems as they move through the acquisition lifecycle. Adaptable systems, however, do not move through the acquisition lifecycle in a linear way. They are almost constantly engaged in development, production, and sustainment simultaneously. While it is entirely possible for programs to budget multiple colors of money at the same time, it is almost inevitable with adaptable systems that these budget estimates will not keep pace with program developments creating the need for constant reprogramming of funds.

The multifunctionality of adaptable systems is also a major challenge for a budget process that organizes around distinct program offices and organizational lines of responsibility. A multifunctional adaptable system is difficult to procure in an acquisition and budget system accustomed to handling major functions such as communications, battlespace awareness, and electronic warfare as separate systems, procured by separate offices, using separate budgets.

Misaligned Business Incentives

Business incentives for industry can be misaligned for adaptable systems. Prime contractors derive their return on investment from anticipated work shares and the integration of known technologies. Configuration and design churn from adaptable systems could undermine prime contractor profitability and also create business uncertainty for first and second tier subcontractors whose business may be displaced. Additionally, defense prime contractors complain that adoption of iterative development methods is hampered by DoD contract requirements of documentation, milestone reviews, and incentives based on traditional waterfall-based models (Defense Science Board, 2018).

Rigid contract structures, such as fixed price development contracts, are a substantial barrier to the development of adaptable systems. Because these contract structures create powerful incentives for the government and the contractor to try to stick to the original contract terms to the letter, the ability to dynamically reshape program content and add capability is effectively precluded.

As RAND’s Jonathan Wong (2016) has noted,

> If the Pentagon wants to reproduce the speedy results of rapid acquisition programs in peacetime, it must find more direct and efficient ways to determining effectiveness that involve the operational user earlier—and not penalize the contractor and the military for going back to the drawing board when something does not work.

Lack of In-House Technical Expertise

Both in-house technical expertise as well as external partners are essential for adaptable systems in delivering the technical level of software engineering needed as well as establishing appropriate requirements for software functionality. The DoD has struggled to acquire top software talent, which makes it difficult for all parties to speak in a common language and communicate software-based problems, as well as interact effectively with developers and testers to communicate needs, understand opportunities, and test performance. This has made it challenging to plan for and takes time to deploy upgrades to operating fleets and to train personnel on how to use them. Software-based systems not only require the necessary software talent but also the understanding of process and expectations from both commanders and policymakers. Finally, even as new systems are built to incorporate adaptability, the DoD is faced with the challenges of backward compatibility, cross-system interoperability, and increased variation in existing systems. This complicates both training and sustainment.

Section 4: Enablers

A variety of enablers exist to overcome or mitigate these barriers. Overall, these enablers encourage earlier and more rapid testing, flexibility in funding, requirements and new designs that are base platform/open architecture with ability to add on new, interoperable software-based payloads/capabilities that are each advancing with iterative and continuous development. They must also incorporate distributed, continual, and agile testing based on shared core architecture to make sure each update is integrated effectively, does not interfere with other component.

MOSA and Adaptable Architecture

MOSA enables adaptable systems by easing the process of integrating and replacing subsystems and components, as well as enabling flexibility, competition, and opportunities for distributed development. Architectures that are designed for adaptability from the ground-up make flexibility easier. This includes building systems that can easily incorporate new software-defined capabilities. MOSA should be a baseline expectation whenever a system will require adaptability.

Army Major General Bruce T. Crawford has explained that “the industrial base that supports the Department of Defense has been using software to modernize, instead of focusing on just hardware as the mechanism by which they've been able to increase capability.” Software modernization in an open-architecture environment enabled this approach (Osborn, 2017).

Open standards allow for many different developers to contribute to a system over time, regardless of whether they were involved in the initial system development. This allows for more freedom of innovation and application due to dispersed development. According to Nick Guertin, senior software systems engineer at the Carnegie Mellon University Software Engineering Institute, MOSA “has helped the Defense Department improve its buying power. It opens up the market opportunities for the greatest possible number of buyers” (Brust, 2018).

In addition, MOSA can help outline possible modernization paths going forward. Maj Gen Zabel said,

> Open mission systems is a requirement for how every new system is built … and we are finding that it’s been a great advantage in not only opening us up immediately to a larger part of the industrial base, but also giving us … a step by step modernization path. (Owens, 2017)

Incremental and Iterative Development

A variety of tools for incremental and iterative development can be adopted for software-based systems. These include the adoption of commercial software development techniques, such as agile development, DevOps, and development sprints, which enable adaptable systems by providing a foundation for iterative change and reducing, especially if combined with oversight regimes that eliminate the rigid predictability demands of the current acquisition system. Software-defined systems, if built for flexibility and adaptability, can prolong the effective lifecycle of their base hardware platforms while lowering cost of technology currency and potentially simplify hardware sustainment through reduced obsolescence.

According to Vice Admiral Mat Winter, Program Executive Officer for the F35,

> The current acquisition strategy has us doing a serial [and] sequential design, develop, integrate, test [and] deliver strategy. I’m not convinced that’s the most efficient and effective way, most importantly, to deliver and continuously deliver capability to our war fighters … as we go beyond Block 3F.

Winter has worked to develop more of an adaptable systems approach to F-35 upgrades as part of the continuous development and delivery approach. “I am going to be asking the system to do things it’s never done before,” he said. “I’m asking the system to do true model-based systems engineering simultaneously with capabilities-based testing. The same time. With DT [developmental testing] and OT [operational testing happening at the] same time. Real time. Allowing us to be able to truly change the way we contract and cost estimate” (Insinna, 2017).

Increased User Feedback and Testing

Increased user feedback is necessary for software-based adaptable systems to both improve the functionality of the system, as well as incorporate the desired changes in real time. Increased feedback loops, a critical part of the agile process, will make sure the product that is delivered is the product the warfighter actually needs. This means increased use of things like prototyping, which provides real-time testing of systems in warlike environments, and expanding the use of virtual twin testing, where deployed systems can take real-time data and interact in real-time environments. For example, the Navy currently uses versions of virtual twin testing for its combat systems “so that new technologies can be tested by the crew and commanders before its uploaded into the main combat system, a hedge against reaping unintended consequences by uploading a feature or patch without knowing exactly how it will fit into the ship’s systems” (Larter, 2018). The army has implemented the use of beta-testing squadrons in order to field systems in real environments in Europe as well (Pawlyk, 2017). The air force is using a virtual twin prototyping approach for its program to reengine the B-52 bomber (Mayfield, 2019).

Increasing user feedback has a number of benefits. It recognizes that requirements and perceived optimal design may not actually operate as expected or anticipated. Additionally, this process encourages innovation among developers and the user community. “Maybe all the requirements aren’t met at the first go, but you have something that you can put in the hands of the operator and they can use it,” explained Air Force General Ellen Pawlikowski. “Once you put it in the hands of the operator, maybe some of the requirements you had in the beginning don’t make sense anymore, because [operators] see how they can actually use it and requirements change” (Owens, 2017). This means the traditional system to create test and evaluation as a separate phase from development is incompatible with iterative development. Even as systems are fielded, they will always be in a state of evaluation and upgrade. Air Force Maj Gen Zabel states, “In order to do that you need to integrated development and test to make sure that what you’re delivering to the field is actually worth delivering to the field” (Owens, 2017).

Finally, faster user feedback and real-time testing assists in developing software that can adapt to new environments and problems are emerging in close-to real time. Currently, the feedback time for warfighters to deliver input back from the field is too long to incorporate the changes into software in a timely manner. The DoD is therefore losing an opportunity to gain advantage.

Budgeting for Adaptable Systems and Flexible Funding

Budgeting for adaptable systems involves multiple aspects. In the first instance, it means budgeting within programs with the recognition that an adaptable system will not make a linear progression through development to production to sustainment. Rather, the program will be involved simultaneously in all three phases, with funding to support continuous software development remaining at a fairly constant level throughout most of the system’s lifecycle. Different services have adopted different budgeting strategies for software development, but the need to adopt budget mechanisms to support this is consistent across the DoD (McQuade, 2019, pp. 31–32).

The Defense Innovation Board has specifically recommended a new category of appropriation for software that would cover software activities currently funded variously through the operation and maintenance; procurement; and research, development, test, and evaluation appropriations (McQuade & Murray, 2019). Such a new appropriation would provide substantial flexibility in funding software development and fielding needs with a minimum of process friction compared to today's budgeting system. Existing tools could also be modified to reduce the friction currently caused by the need to reprogram funds from one appropriation to the another to facilitate agile software development. Helpful measures include clarifying and narrowing the definition of new starts, reducing the rigidity in colors of money so that reprogramming requests are less often necessary, broadening budget justification language to cover broader scopes for research and development, and providing more readily used mechanisms for adjusting color of money.

Budgeting for adaptable systems can also mean creating programmatic space outside of MDAPs for maturing subsystem technologies that may have application across multiple platforms. Congress provided a potential framework for this approach in the National Defense Authorization Act (NDAA) for Fiscal Year 2017 by creating funds in each service for subsystem and component development and prototyping (NDAA, 2016). This approach would allow the military services to budget significant funding for research and development for technologies not directly associated with a program of record (and therefore likely not tied to a program of record requirement). Currently, the Small Business Innovative Research program is one of the only significant sources of R&D funding outside of programs of record, but the SBIR program is not accessible to firms that are not small businesses. Increased use of portfolio-based acquisition management may also be an enabler for more technology development outside of MDAPs (ACT-IAC, 2019). The Section 809 panel records managing acquisition more on a broad portfolio basis rather than focusing on individual programs of record. Such an approach could allow for technology developed in a portfolio to be adopted widely among adaptable systems within the portfolio.

Contracting Mechanisms

Contracting mechanisms that best support adaptable systems are likely to be those that foster collaboration between the government and the prime contractor. The more collaboration there is in this relationship, the less effort that is required to establish tight specifications for every aspect of work. This suggests that it would be challenging, if not impossible, to carry out an adaptable systems program in a fixed price for development contracting model. Other Transaction Authority agreements (OTAs) and flexible contracting mechanisms, such as multiple award IDIQs, can allow for more flexibility in contracting for adaptable systems that can readily add and subtract work scope as needed. In cases where the collaboration may require coordination across large elements of an industrial sector the use of consortia and alternative competitive constructs may facilitate the coordination and continuous evolution of requirements throughout the acquisition process.

The Section 809 Panel recommendations for acquisition of technology that is readily available, and readily available with modification, can facilitate contracting for adaptable systems (ACT-IAC, 2019). Similarly, the Defense Innovation Board has proposed a streamlined authority creating software acquisition pathways that can provide a useful mechanism for adaptable systems, particularly for systems that were not original set up to be adaptable systems that are transitioning toward an adaptable systems structure (McQuade & Murray, 2019).

Dynamic Marketplace

A dynamic marketplace approach to working with industry, especially in acquiring technology with strong commercial elements, is recommended by the congressionally mandated panel on acquisition streamlining, also known as the Section 809 Panel (ACT-IAC, 2019). The dynamic marketplace approach involves fostering competition by obtaining proposals from industry prior to establishing discrete performance requirements. The goal of this approach is to leverage commercial innovation and non-traditional partners, placing military mission at the center of government/industry dialogue. Industry consortia can be a good enabler for many of these discussions. The dynamic market place approach can support adaptable systems by encouraging commercial practitioners of agile software development approaches to participate in defense acquisition and by reducing the impetus to define highly detailed performance requirements at the front end of acquisition programs.

Functionally-Aligned Workforce and Increased Training in SW Expertise

A functionally-aligned workforce and increased training in software expertise will also enable leadership and understanding of the opportunities posed by adaptable systems. With leadership buy-in, the DoD can specify technical career tracks, adjust for competitive talent acquisition, cross-service collaboration, develop a broader knowledge across the Department of Technology and offer competitive compensation for potential applicants.

Air Force Chief Technology Officer Frank Konieczny has discussed how the human element is a major factor in the success of agile software development in the Air Force. Turnover in the work force and challenges in tracking programming skills as part of a career field when making assignments make it difficult to have personnel continuity and the right mix of skills in pursuing agile software development (Williams, 2018).

The DoD must enhance its talent by both leveraging current expertise as well as attracting and retaining new talent. Specifying technical career tracks and establishing competitive compensation will significantly help. According to the NDS, the DoD plans to “emphasize new skills and complement our current workforce with information experts, data scientists, computer programmers, and basic science researchers and engineers—to use information, not simply manage it” (DoD, 2018).

Issues with the workforce are not limited to dealing with the development and management of software expertise among those writing and working directly with software. As emphasized in the workforce recommendations of the Defense Science Board study on software acquisition, the DoD also needs to increase software awareness and understanding among program managers and program executive officers as well as in managers in industry (Defense Science Board, 2018). Establishing a culture supportive of adaptable systems will take time and will entail taking a different view of risk. According to DIUx Managing Partner Raj Shah, “For us internally, if a team or project team really stretches to try a technology or approach that’s really novel but there’s technical risk involved … technology risk is acceptable and for a certain level we encourage it” (Carberry, 2017).

Section 5: Overall Strategy

While the enablers required for adaptable systems already exist and do not necessarily need new authorities to be implemented, actually combining these tools in an effective and coordinated way remains difficult. It is ultimately essential to understand how these enablers work together and begin a larger environmental transition toward their use. While elements across the DoD are taking steps to implement a variety of the enablers listed above, the use of many of them is still comparatively rare and it is even rarer to see several of them used together.

In order to achieve success in the acquisition of adaptable systems, the DoD may consider the creation of a clearly defined adaptable systems lane. The DoD currently describes its Adaptive Acquisition Framework as one that includes a variety of approaches including the Section 804 Middle Tier of Acquisition approach, rapid acquisition, and traditional acquisition. This framework could be expanded to include an adaptable systems lane as well. Systems in the adaptable systems lane would default to the use of the enablers described above rather than using them by exception. More traditional approaches could still be used, but they would be the exceptions in the adaptable systems lane. If an adaptable systems lane were created, however, it would be important to ensure that it not monopolize the use of these enablers. The goal of this effort is to enhance the ability of program managers and other acquisition leaders to appropriately use the right tools to acquire adaptable systems, not to impose limitations or straightjackets on them.

Conclusion

Deploying systems that are adaptable and agile is not just a technology strategy, but a security imperative. Success will ultimately depend on the DoD's ability to adjust rapidly to uncertainty in threats—nimble adversaries, new domains, and unanticipated applications of technology utilizations. Our current acquisition debate is currently failing to directly address the changing nature of what we need to be buying, and as a result, we may be heading towards another round of acquisition reform recriminations in a few years. A successful approach to adaptable systems requires using the enablers identified in this report to overcome the barriers to adaptable systems.

References

ACT-IAC. (2019, January 16). *Report of the advisory panel on streamlining and codifying acquisition regulations, Volume 3, DoD 809 panel.* Retrieved from https://www.actiac.org/report-advisory-panel-streamlining-and-codifying-acquisition-regulations-volume-3-dod-809-panel

Brust, A. (2018, September 11). *Open systems evolving to improve DoD buying power.* Retrieved from https://federalnewsnetwork.com/open-systems-2018/2018/09/open-systems-evolving-to-improve-dod-buying-power/

Carberry, S. D. (2017, March 21). *DIUx head wants to drive culture change at DoD.* Retrieved from https://fcw.com/articles/2017/03/21/diux-innovation-carberry.aspx

Defense Industry Daily staff. (2019, February 11). *USN ship protection: From "Slick 32s" to SEWIP*. Retrieved from https://www.defenseindustrydaily.com/us-navy-from-slick-32s-to-sewip-05365/

Defense Science Board. (2018, February). *Design and acquisition of software for defense systems.* Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/1048883.pdf

DeLuca, P., Predd, J., Nixon, M., Blickstein, I., Button, R., Kallimani, J., & Tierney, S. (2013, May 3). *Assessing Aegis program transition to an open-architecture model.* Retrieved from https://www.rand.org/pubs/research_reports/RR161.html

DoD. (2015, January 7). *Operation of the Defense Acquisition System.* Retrieved from https://www.dau.mil/guidebooks/Shared Documents/DoDI 5000.02.pdf

DoD. (2018). *Summary of 2018 National Defense Strategy*. Retrieved from https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Durbin, J., & Scharadin, R. (2011, May 18). *The modernization of the Aegis fleet with open architecture.* Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a557871.pdf

Freedberg, S. (2016, November 3). Navy forges ahead with new surface ship electronic warfare: SEWIP. Retrieved from https://breakingdefense.com/2015/03/navy-forges-ahead-with-new-surface-ship-electronic-warfare-sewip/

Gallagher, S. (2012, June 18). How to blow $6 billion on a tech project. Retrieved from https://arstechnica.com/information-technology/2012/06/how-to-blow-6-billion-on-a-tech-project/2/

Gallagher, S. (2018, March 8). The Army's costly quest for the perfect radio continues. Retrieved from https://arstechnica.com/information-technology/2018/03/the-armys-costly-quest-for-the-perfect-radio-continues/

Hlad, J. (2017, February 2). More BACN, please. Retrieved from http://www.airforcemag.com/Features/Pages/2017/February 2017/More-BACN-Please.aspx

Insinna, V. (2017, September 6). F-35 program office floats new "agile acquisition" strategy. Retrieved from https://www.defensenews.com/smr/defense-news-conference/2017/09/06/f-35-program-office-floats-new-agile-acquisition-strategy/

LaGrone, S. (2015, February 12). Navy awards SEWIP Block III contract to Northrop Grumman. Retrieved from https://news.usni.org/2015/02/12/navy-awards-sewip-block-iii-contract-northrop-grumman

Larter, D. B. (2018, September 26). On the new battlefield, US Navy must get software updates to the fleet within days, acquisition boss says. Retrieved from https://www.c4isrnet.com/digital-show-dailies/modern-day-marine/2018/09/25/on-the-new-battlefield-the-navy-has-to-get-software-updates-to-the-fleet-within-days-acquisition-boss-says/

Mayfield, M. (2019, February 28). Air Force to release RFP for B-52 re-engining program. Retrieved from http://www.nationaldefensemagazine.org/articles/2019/2/28/air-force-to-release-rfp-for-b52-reengining-program

McQuade, M., & Murray, R. (2019, March 21). *Software is never done: Refactoring the acquisition code for competitive advantage.* Retrieved from https://media.defense.gov/2019/Mar/26/2002105909/-1/-1/0/SWAP.REPORT_MAIN.BODY.3.21.19.PDF

Military and Aerospace Electronics. (2004, December 1). Software-defined radio and JTRS. Retrieved from https://www.militaryaerospace.com/articles/print/volume-15/issue-12/features/special-report/software-defined-radio-and-jtrs.html

National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328 (2016, December 23). Retrieved from https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf

Northrop Grumman. (n.d.). Battlefield Airborne Communications Node (BACN). Retrieved from http://www.northropgrumman.com/Capabilities/BACN/Pages/default.aspx

Osborn, K. (2017, February 27). Army convenes key parties to discuss software in modern weapons. Retrieved from https://defensesystems.com/articles/2017/02/27/solarium.aspx

Owens, K. (2017, July 14). Agility is the future of software development, says Air Force general. Retrieved from https://defensesystems.com/articles/2017/07/14/air-force-cybersecurity.aspx

Owens, K. (2017, November 17). Air Force pushes faster, more agile IT acquisition. Retrieved from https://defensesystems.com/articles/2017/11/17/air-force-it.aspx

Pawlyk, O. (2017, October 9). *Army weapons tests on the fly in effort to win race against Russia.* Retrieved from https://www.military.com/daily-news/2017/10/09/army-weapons-tests-fly-effort-win-russia.html

Pearn, M. (2008, November 12). Seek and destroy: The Aegis combat system. Retrieved from https://www.naval-technology.com/features/feature45460/

U.S. Navy. (2017, January 30). Surface Electronic Warfare Improvement Program (SEWIP). Retrieved from https://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=475&ct=2

U.S. Navy. (2019, January 10). AEGIS weapon system: Fact file. Retrieved from https://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=200&ct=2

Williams, L. C. (2018, October 3). Air Force wants to make “Kessel Run” standard in tech acquisition. Retrieved from https://fcw.com/articles/2018/10/03/usaf-kessel-run-standard.aspx

Wong, J. (2016, June 23). Don’t learn the wrong lessons from rapid acquisition. Retrieved from https://www.defenseone.com/ideas/2016/06/dont-learn-wrong-lessons-rapid-acquisition/129332/

About CSIS

For more than 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world’s greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decision-makers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, DC. The Center’s 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world’s preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center’s president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgements

The authors of this study relied upon feedback received at two workshops held at CSIS as well as discussions with other knowledgeable individuals in industry and the defense acquisition community. Particularly important were discussion held with the staff of the Defense Innovation Board engaged in the Software Acquisition and Practices Study.

This CSIS study was made possible by the support of Northrop Grumman.

Acquisition System Design Analysis for Improved Cyber Security Performance

Brad R. Naegle, LTC, U.S. Army (Ret.)—is a Senior Lecturer at the Naval Postgraduate School, Monterey, CA. In addition to acquisition course development and delivery, he is a member of the Navy's software community of practice. While on active duty, LTC (Ret.) Naegle was assigned as the Product Manager for the 2½-ton Extended Service Program (ESP) and USMC Medium Tactical Vehicle Replacement (MTVR) from 1994 to 1996 and served as the Deputy Project Manager for Light Tactical Vehicles from 1996 to 1997. He was the 7th Infantry Division (Light) Division Materiel Officer from 1990 to 1993 and the 34th Support Group Director of Security, Plans, and Operations from 1986 to 1987. Prior to that, LTC (Ret.) Naegle held positions in test and evaluations and logistics fields. He earned a Master of Science degree in systems acquisition management (with Distinction) from the Naval Postgraduate School and an undergraduate degree in economics from Weber State University. He is a graduate of the Command and General Staff College, Combined Arms and Services Staff School, and Ordnance Corps Advanced and Basic Courses.

Abstract

There is ample evidence that cyber-attacks and cyber warfare are a growing concern for the United States. Our warfighting systems and networks have inherent vulnerabilities and so are targets for cyber adversaries. By nature, cyber warfare is an asynchronous strategy, so the danger posed by a cyber threat is not proportional to the size of the entity initiating the attack. The United States' traditional adversaries, state and non-state actors, domestic terrorists, and even individuals can pose an equally dangerous threat.

The various types and astonishing number of cyber-attacks on the DoD has focused efforts to limit exposure to cyber-attacks and mitigate unavoidable vulnerabilities. The most effective way to "harden" systems against potential cyber-attacks is to develop the system with a cyber warfare mindset. To do this, program managers must have an in-depth understanding of their system's cyber vulnerabilities and exercise control over the design and configuration of those vulnerable subsystems.

There are several challenges in both understanding and controlling a system's cyber vulnerabilities, including that the Defense Acquisition System (DAS) is designed to cede most of the design decisions to the contractor. All known and potential cyber vulnerabilities need to be treated as system Configuration Item, so that design and configuration is under government control.

Fortunately, there are tools, techniques, and analyses that can augment the DAS to gain a better understanding and provide more control over the design and configuration of those subsystems presenting cyber vulnerabilities. This research analyzes the integration of these tools and the expected improvement in cyber performance resulting from the implementation. The tools include the integration of the Maintainability, Upgradeability, Interoperability, Reliability, and Safety/Security (MUIRS) analyses; Software Engineering Institute's Quality Attribute Workshop (QAW); Software Engineering Institute's Architecture Trade-off Analysis Methodology^{sm}; and the Failure Modes and Effects Criticality Analysis (FMECA).

Background

Hardly a day has gone by during my tenure at Cyber Command that we have not seen at least one significant cybersecurity event occurring somewhere in the world. We face a growing variety of advanced threats from actors who operate with ever-more sophistication and precision. —Admiral Michael S. Rogers, Commander, U.S. Cyber Command (Pellerin, 2017)

Threats from cyber-attacks have clearly emerged as one of the most significant threats to the United States and to the Department of Defense (DoD). The sources of attack are varied and include state and non-state actors, traditional adversaries, as well as domestic sources. The emergence of artificial intelligence (AI) cyber-attacks has added to the threat significantly. “Automation and artificial intelligence are beginning to ‘make profound changes to the cyber domain,’ a threat that the military hasn’t yet fully grasped how to counter, Robert Behler, the Defense Department’s director of operational test and evaluation, said” (Capaccio, 2019).

Cyber-attack is an extremely effective, asynchronous warfare tactic, meaning that adversaries that could not possibly face the U.S. military can still be very effective in the cyber environment. While traditional adversaries like China, Russia, North Korea, and Iran are certainly players in the cyber-warfare arena, non-state actors, domestic terrorists, and even individuals can pose a disproportionate threat in the cyber world.

> The relatively inexpensive cyber options being employed today by both state and non-state hacking groups make it an incredibly efficient “leveler” of power. A small group of hackers using simple spear-phishing tactics, for example, can have massive impact on military installations, government operations, critical infrastructure and potentially even weapons systems. (Martini, 2016)

Obviously, this opens up the cyber-threat adversaries list to an unimaginable number that would be nearly impossible to manage or even prioritize.

The types and sophistication of cyber-attacks are growing exponentially. Denial-of-Service (DoS) or Directed-Denial-of-Service (DDoS) attacks have impacts on communications, networks, internet, intranet, and systems using Global Positioning System (GPS) to name a few. Malicious software (malware) is a common cyber-attack methodology that can take several forms from passive collection of data to destructive applications designed to destroy or disrupt operating systems. Spoofing is the introduction of erroneous or misleading information into systems that can dramatically affect operations and can even include voice or video communications assembled by AI that appear to be authentic, but are compilations from available sources. Can you imagine getting verbal commands in the recognized voice of the commander that are realistic in appearance, but totally constructed by AI? Take-over of systems is certainly of concern and in 2011, Iran claimed that it took over a U.S. RQ-170 surveillance drone, although that is disputed by the United States. It was not clear how Iran acquired the drone intact. Some U.S. experts dismiss the possibility that Iran could hack and then take over the drone’s controls, as Iran claims. And yet similar disruptions have proven possible in other battlefields, notably with the Iran-backed Hezbollah militia in Lebanon and drones from Israel.

> “Those jamming capabilities exist, and a lot of them are not as new as we would like to imagine,” says former U.S. Navy electronics warfare officer Densmore. “Anything that has a sensor, that takes communications links—as does the RQ-170, which has two, one for the satellite, and the other is line-of-sight with the ground control station—all it takes is disrupting that.” (Peterson, 2011)

In 2015, the FBI filed a report regarding a United Airlines passenger who had repeatedly gained engine thrust controls of Boeing 737 airliners through the entertainment port:

> During the conversations, [FBI investigating special agent Mark] Hurley wrote, [Chris] Roberts disclosed that he had previously hacked into IFE [in-flight entertainment] systems, manufactured by Panasonic and Thales—which provide video monitors in the passenger seatbacks—about 15 or 20 times on various flights between 2011 and 2014. According to the document, Roberts said he gained access to the systems by plugging his own laptop computer into the IFE system's electronic boxes mounted under passenger seats. Once in the system, he said he was able to access other systems—including the jets' Thrust Management Computer, which is responsible for providing power to the plane's engines. (Ware, 2015)

Software hacking with active systems designed to destroy, take over, or spoof software applications have exploded. In addition, stealthy software attacks designed to gather data, log keystrokes, or lay in wait for a particular event, peer connection, or timing event are more and more common. In short, there appears to be no end to the types of cyber-attacks or the combinations and permeations of those known today.

The methods for conducting cyber warfare appear to be continuing to expand, and with AI-generated attacks, the differing types of attacks are likely to continue to expand. The proliferation of types of cyber-attacks was one of the drivers for the transition from the Defense Information Assurance Certification and Accreditation Program (DIACAP), which tended to be a terminal process once the certificate was issued, to the Risk Management Framework (RMF), which is a continuous risk management process. While this is a logical approach given the constantly advancing cyber threats, it causes more work for the PM as the iterative process will be examined numerous times during the developmental process.

DoD Acquisition Cyber Exposure

An ever-increasing number of DoD weapon systems are leveraging technology that, unfortunately, places them in danger of cyber-attacks. The DoD's warfighting systems have degrees of dependence on GPS, communications, networks, and software, which all have opportunities for cyber vulnerabilities. The DoD is in the process of developing more extensive networks to leverage the inherent advantages with the communication capabilities, as well as the situational awareness that networks can provide. These more extensive networks will include more and more platforms, thus increasing their cyber vulnerabilities, as well. All of these will be extremely valuable cyber targets for adversaries. The advantages of the system technologies and networks will continue to be desired by the DoD, so planning effectively to counter cyber vulnerabilities will be a reality for system and network developers.

This all means that the DoD will continue to develop systems and networks with inherent cyber vulnerabilities, managing those vulnerabilities with a continuous RMF process. This puts the program manager (PM) in a nearly constant state of cyber vulnerability assessment, reacting to the ever-emerging cyber threats from the vast array of entities involved in cyber warfare against the United States. This could potentially require significant time and resources to track and assess every emerging cyber threat and perform a vulnerability assessment on the system under development.

The PM cannot control the emergence of new cyber threats, so must concentrate on what can be controlled: the system's cyber vulnerabilities. Understanding the system's vulnerabilities allows the PM to quickly and efficiently assess any new cyber threat and quickly perform an RMF iteration to verify the severity of the threat and any mitigation efforts available. The PM must identify all system potential or actual cyber vulnerabilities and take control of managing the design and architecture of each one. All cyber vulnerabilities must be designated as a Configuration Item (CI), placing it under government control, or at least be treated the same way as a CI.

Barriers to Effective Cyber Performance Design

There are significant barriers to achieving a complete understanding of any system's vulnerabilities, but overcoming these barriers is a key to being able to rapidly respond to new cyber threats. Any communications conducted by the system are a potential vulnerability, but especially wireless communications such as those used by unmanned aerial vehicles (UAVs), transmitting intelligence, surveillance, and reconnaissance systems, systems using GPS or other guidance/positioning information, and many autonomic systems that passively transmit system health data. While this seems to be rather straight forward, some commercial components may have communications abilities that are not apparent. For example, virtually all cell phones include an FM radio chip that can be activated: "That's right; today's smartphones have a built-in FM chip that gives them the ability to receive radio signals in your area" (OPB, n.d.). An in-depth understanding of any subsystem capable of transmitting or receiving information is required.

System software development is a particular challenge in ensuring that any cyber vulnerability is known. The software must be engineered carefully to minimize vulnerabilities, and significant design and engineering needs to be included for software-intensive systems to be able to self-check for cyber intrusion attempts. For example, cyber vulnerabilities could be significantly reduced if the software application could detect and immediately report any attempt to modify or add software lines of code, or access to system software at all. Any authorized access or maintenance activities would need to have a rigorous authentication protocol to ensure only authorized access or changes were accepted.

Software engineering needs to be conducted with cyber vulnerabilities as a hard parameter. One of the challenges in software engineering is to keep the software from communicating and interacting with other connected software systems or modules. The Boeing 737 example of accessing flight controls through the entertainment system is a good example of this concept. With all of the engineering discipline needed to reduce cyber vulnerabilities, using commercial software or reused software is extremely problematic, if not impossible. Any existing software to be added to the architecture of a developmental system would have to be thoroughly vetted and the inner working known to a very high degree. With most commercial software, this is not possible as the DoD does not own the data rights and they are most often not obtainable because there is so much of the commercial company's proprietary practices evident in the code. In addition, there are a significant number of coders who code in what is known as a "back door" to the software that allows them access, bypassing the normal security protocols built into the programs.

> The National Grid could be at risk of a cyber attack after a hacker group linked to China create a "back door" in software used by big businesses. Companies at risk from this latest attack include American weapons firm Lockheed Martin, Russian energy supplier Gazprom and French bank Société Générale. (Tarrant-Cornish, 2017)

This means that software reuse and using most commercial software would be nearly impossible when considering potential cyber vulnerabilities unless the engineering structure was completely known and verified to ensure that any potential cyber vulnerabilities associated with the reused code were understood and included in the risk management. While this seems logical, the amount of software engineering needed to achieve this in the reused software may actually exceed the engineering effort in the original design and build of the app. Again, this presupposes that the original software is even accessible, which is not the case in most commercial software.

The Challenge

The PM must have control and insight to the system architecture, build processes, and verification methodologies that far surpasses the current state of practice in the DoD acquisition environment to gain control of known and future cyber threats.

This challenge is exacerbated by the existing DoD acquisition environment for developing systems.

> Since the implementation of Acquisition Reform in the nineties, detailed specifications have been replaced with performance specifications in order to leverage the considerable experience and expertise available in the defense contractor base. In most hardware-centric engineering disciplines, the expertise that the DoD seeks to leverage, includes a mature engineering environment in which materials, standards, tools, techniques, and processes are widely accepted and implemented by industry leaders. This engineering maturity helps to account for derived and implied requirements not explicitly stated in the performance specification. (Naegle, 2014, p. 8)

The DoD requirements generation system has been designed to provide the contractor with performance specifications to be met within some parameters. In short, the design control and engineering has been placed in the hands of the contractor to leverage the advancements obtained in the commercial sector. In the current and rapidly advancing cyber warfare environment, the DoD now finds that it needs to have much more positive control of the engineering design and build processes that it had significantly ceded to the contractor.

A Way Forward

Fortunately, there are existing analyses, tools, and techniques that can augment the Defense Acquisition System (DAS) to gain more insight and control over the critical cyber design elements. I have previously researched several of these and integrated them into the DAS.

Tools, Techniques, and Processes

The tools, techniques, and processes are briefly described as follows.

- The Software Engineering Institute’s (SEI’s) Quality Attribute Workshop (QAW)
- The Maintainability, Upgradability, Interoperability, Reliability, & Safety and Security (MUIRS) analytic technique
- The Software Engineering Institute’s Architectural Tradeoff Analysis Methodology (ATAM^{sm})
- The Failure Modes and Effects Criticality Analysis (FMECA)

Quality Attribute Workshop (QAW)

The QAW is primarily a method for more fully developing system software requirements and is intended to provide stakeholders’ input about their needs and expectations from the software (Barbacci et al., 2003, p. 1). As the system requirements are developed, software quality attributes are identified and become the basis for designing the software architecture. By adding in the desired system cyber performance as a system quality attribute, software design activities will necessarily include analyses of possible system cyber vulnerabilities as part of the design process.

The Software Engineering Institute's (SEI's) Quality Attribute Workshop (QAW) is implemented before the software architecture has been created and is intended to provide stakeholder input about their needs and expectations from the software (Naegle, 2007). The QAW process provides a vehicle for keeping the combat developer and user community involved in the DoD acquisition process, which is a key goal of that process. In addition, the QAW includes scenario-building processes that are essential for the software developer to design the software system architecture (Barbacci et al., 2003, pp. 9–11). These scenarios will continue to be developed and prioritized after contract award to provide context to the quality attribute identified for the system.

Although the QAW would certainly be useful after contract award, conducting the workshop between combat developers/users and the program management office before issuance of the Request for Proposal (RFP) would provide an improved understanding of the requirements, including cyber performance, enhance the performance-specification preparation, and improve the ability of the prospective contractors to accurately propose the cost and schedule. This approach would support the goals of the System Requirements Review (SRR), which is designed to ascertain whether all derived and implied requirements have been sufficiently defined (Naegle & Petross, 2007, pp. 5–6).

The QAW process is primarily designed to more fully develop system software requirements so that the government Request for Proposal (RFP) is clearer to potential contractors. In turn, the resulting proposals should be more accurate and realistic, reducing requirements and project scope creep. This is critical in communicating the cyber security expectations of the system so that they remain a priority when designing the system (Naegle, 2014, p. 25).

Maintainability, Upgradability, Interoperability/Interfaces, Reliability, and Safety/Security (MUIRS) Analytic Technique

The MUIRS analytic technique is designed to provide a framework for better understanding of essential supportability and safety/security aspects that the warfighter needs and expects, but often doesn't communicate clearly with the capabilities-based JCIDS documents. This analytic technique helps compensate for the immature software engineering environment as the MUIRS analysis illuminates the derived and implied requirements that the immature environment cannot (Naegle, 2014, p. 25).

Much of the software supportability and safety/security performance that typically lacks consideration and is not routinely addressed in the software engineering environment can be captured through development and analysis of the MUIRS elements. Analyzing the warfighter requirements in a QAW framework for performance in each MUIRS area will help stakeholders identify software quality attributes that need to be communicated to potential software contractors (Naegle, 2006, pp. 17–24). The system safety and security (the "S" in MUIRS) would certainly address the cyber performance and vulnerabilities as part of the analysis process. The MUIRS analysis assists the QAW process by focusing on those elements that are, too often, overlooked during the requirements generation process.

MUIRS primarily addresses the immature software engineering environment as it provides an analytic approach for critical sustainment and safety/security attributes that are often missing, weakly articulated, or vaguely stated in the requirements produced. With its capabilities and performance-based requirements processes, the DoD significantly depends on mature engineering environments to "fill the gaps" left from the requirements generation and communication processes, but the software engineering environment is unable to do so.

The MUIRS analysis is also an enabler for the QAW and ATAM^{sm} architectural processes discussed next (Naegle, 2014, p. 25).

Architectural Tradeoff Analysis Methodology (ATAM^{sm})

The Software Engineering Institute's Architectural Trade-off Analysis Methodology ATAM^{SM} (ATAM) is an architectural analysis tool designed to evaluate design decisions based on the quality attribute requirements of the system being developed. The methodology is a process for determining whether the quality attributes are achievable by the architecture as it has been conceived before enormous resources have been committed to that design. One of the main goals is to gain insight into how the quality attributes trade-off against each other (Kazman et al., 2000, p. 1). Obviously, the system's capabilities will necessarily be traded off with their inherent cyber vulnerabilities as part of the ATAM process. Those unavoidable cyber vulnerabilities will then need to be mitigated throughout the design of the system.

Within the Systems Engineering Process (SEP), the ATAM provides the critical Requirements Loop process, tracing each requirement or quality attribute to corresponding functions reflected in the software architectural design. Whether ATAM or another analysis technique is used, this critical SEP process must be performed to ensure that functional- or object-oriented designs meet all stated, derived, and implied warfighter requirements. In complex systems development such as weapon systems, half or more than half of the total software development effort will be expended in the architectural design process. Therefore, DoD program managers must ensure that the design is addressing requirements in context and that the resulting architecture has a high probability of producing the specified warfighters' capabilities described in the JCIDS documents, with increasing emphasis on the cyber performance and vulnerabilities (Naegle, 2014, pp. 26–28).

The ATAM focuses on quality attribute requirements, so it is critical to have precise characterizations for each. To characterize a quality attribute, the following questions must be answered:

- What are the stimuli to which the architecture must respond?
- What is the measurable or observable manifestation of the quality attribute by which its achievement is judged?
- What are the key architectural decisions that impact achieving the attribute requirement? (Kazman, Klein, & Clements, 2000, p. 5)

The ATAM is designed to elicit the data and information needed to adequately address the three questions above. These questions, focused on requirements and quality attributes, are user-centric, and so the ATAM scenarios must be constructed by the user community (Naegle & Petross, 2007, p. 25). The methodology keys on scenario development in three main areas:

- Use Case Scenarios. As the name suggests, these scenarios describe how the system will be used and sustained in the harshest environments envisioned. It includes all interoperability requirements and duty cycles as well. These user-created scenarios convey critical cyber performance information to the system developer including who uses it (and how do we know that it is an authorized user), how they use it (does it involve communication, sensors, GPS, automated inputs, software, etc.), how they maintain it (e.g., would software maintenance be done remotely, which would be a huge cyber vulnerability, etc.), how they use it (does any of the use or maintenance create cyber vulnerabilities, what does it interoperate with, etc.), when and for how long they use and maintain it, and of course, all of the known ways that the adversary will attack the system, including cyber.

- Growth Scenarios. Growth scenarios focus on known and anticipated system change requirements over the intended life cycle. These scenarios include upgrades and technology refreshments planned; interoperability requirements, such as inclusion in future warfighting networks; changes in sustainment concepts; and other system changes expected to occur over time. For each growth event impacting a cyber vulnerability component, a full Risk Management Framework iteration should be planned.
- Exploratory Scenarios. Exploratory scenarios focus on operations in unusual or stressful situations. These address user expectations when the system is degraded or operated beyond normal limitations due to emergency created by combat environments. These scenarios would necessarily include operations while under cyber-attacks of all sorts. The exploratory scenarios include Failure Modes and Effects Criticality Analyses (FMECA) to identify the essential functions that must not fail. For the DoD, failure modes must include failures that are adversary induced, so understanding all vulnerabilities and how they might be exploited is essential to these analyses. This would obviously include cyber vulnerabilities of all types, which would become the basis for conducting risk analyses on all future types and modes of cyber-attack.

As important to the software engineers, FMECA also identifies those enhancing functions that should not preclude the system from functioning when that enhancing function is degraded or non-operational. For example, the M1 Abrams tank uses the ambient temperature as an enhancer to the main gun accuracy but needs the ability to be fully operational in the case where the ambient temperature sensor is malfunctioning. The software engineers need that information to properly design the software.

Testing

Test cases are developed out of the scenarios, which firmly link the test program with the user requirements in the context of the scenarios. This methodology also helps to ensure that there are verification events for cyber performance, software, and sustainment requirements, which are too often missing from the testing program (Naegle, 2014).

System cyber testing is extremely challenging, requiring specialized skill sets, such as software hackers, communications and sensor experts, and software engineers, to create software viruses, worms, and the cyber-attack artificial intelligence entities. In addition, significant resources are required to perform some of the cyber-attack scenarios like denial of service attacks. The challenges are exacerbated when combining different types of attacks in the same scenario, as cyber-attacks often do.

It is nearly impossible to keep up with the ever-changing cyber threat environments that should be represented in system testing, and the potential threats created by AI-based cyber-attacks is nearly limitless. This makes it imperative that PMs understand and manage their system’s vulnerabilities, and not simply react to the latest iteration of cyber-attack.

As shown in Figure 1, the ATAM is an integrating function for many of the tools and techniques discussed here. It is designed to be an iterative process and would be most effective when started in early concept development, then continued through contract award, prototyping, and into the design review process.

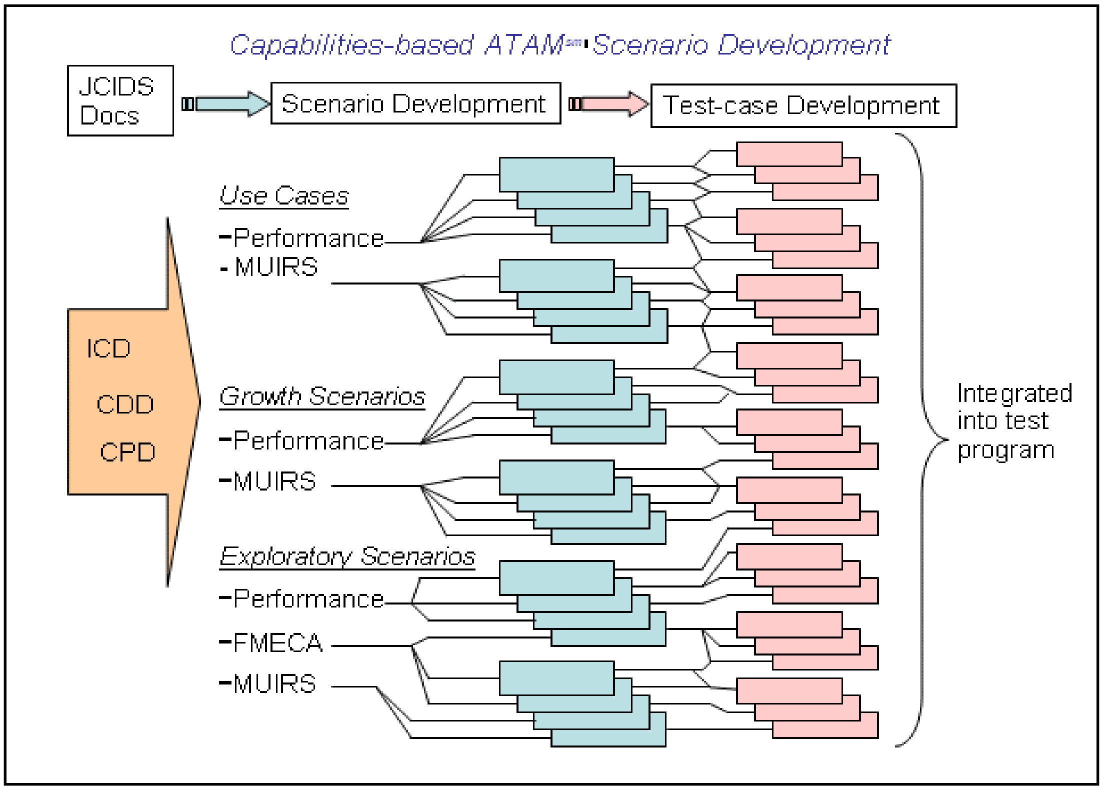


Figure 1. **Quality Attribution Workshop and Architectural Tradeoff Analysis Methodology Integration Into Life-Cycle Management**
(Naegle & Petross, 2007, p. 25)

The ATAM process addresses four primary problem areas:

- The scenario development provides much more operational context than the typical Operational Mission Statement/Mission Profile (OMS/MP) provides. This level of detail helps to compensate for the immature software engineering environment and is critical for the proper design of the software architecture. The details provided by the ATAM scenarios helps to inform system designers to potential cyber vulnerabilities and is critical to the discovery process and optimizing the cyber design.
- The ATAM serves as a very effective software design metric function. With the software development team using 50% or more of the available resources for requirements analysis and software design before the Preliminary Design Review (PDR), it is critical to have an effective software design metrics function. Any significant redesign is extremely costly in both funding and schedule. If the design is reacting to cyber threats, the design process will be in chaos. Traditional software design metrics focus on the design complexity and do not address whether the design is adequate. ATAM directly links the user requirements to the system architectural design.
- As the testing program is developed from the scenarios, it becomes difficult to omit any critical testing event. In addition, the system developer understands the tests or verification events that must be passed for user acceptance. This would feed the Risk Management Framework the valuable information needed to

assess the system’s cyber performance. It would also help identify cyber vulnerabilities and create mitigation actions.

- By integrating the MUIRS analyses into the ATAM scenario development, sustainability and safety/security aspects cannot easily be omitted from the system design. As the testing plan flows from the scenarios, the MUIRS design elements will have corresponding test or verification events identified in the test plan. All of the MUIRS elements need to be considered for cyber vulnerabilities and the safety and security should help drive the cyber performance design (Naegle, 2014, pp. 28–29).

Failure Modes and Effects Criticality Analysis (FMECA)

As the title indicates, this analysis methodology is designed to identify system failure modes, to identify the effects of those failures on the system, and to ascertain the relative criticality of that type of failure. In his book titled *Logistics Engineering and Management*, Benjamin S. Blanchard (2004) describes FMECA as follows:

> Given a description, both in functional and physical terms, the designer needs to be able to evaluate a system relative to possible failures, the anticipated modes and expected frequency of failure, their causes, their consequences and impact(s) on the system overall, and areas where preventative measures can be initiated to preclude such failures in the future. (p. 275)

He goes on to state, “The FMECA is an excellent design tool, and it can be applied in the development or assessment of any product or process” (Blanchard, 2004, pp. 275– 276).

Including ATAM FMECA scenarios with the software systems and subsystems provides architectural design cues to software engineers. These scenarios provide analysis for designing redundant systems for mission-critical elements, “safe mode” operations for survivability- and safety-related systems, and drive the software engineer to conduct “what if” analyses with a superior understanding of failure-mode scenarios. For example, nearly all military aircraft are “fly-by-wire,” with no physical connection between the pilot controls and the aircraft-control surfaces, so basic software avionic functions must be provided in the event of damage or power-loss situations to give the pilot the ability to perform basic flight and navigation functions. Obviously, this would be a major design driver for the software architect (Naegle & Petross, 2007).

The primary problem areas addressed by FMECA include requirements clarification and prioritization, and helping to ensure a sound architecture design. This analysis also ensures that the most critical software systems are designed with the requisite reliability and will continue to function in degraded modes (Naegle, 2014, pp. 29–30).

The user needs to describe what is expected from the system when a cyber-attack occurs. For example, does the system actively counter the attack or merely report the attack to operators? How does the system detect and report passive cyber-attacks? What happens to system operations when remote nodes lose user authentication, and how is connectivity eventually restored? What actions will be taken in a denial of service attack? All known system cyber vulnerabilities need to be included in the exploratory scenarios, as this gives a baseline for reacting to emerging cyber threats.

As previously stated, one of the main functions of performing FMECA is to identify those software functions that are not critical, and to ensure that failures or anomalies in those non-critical functions do not preclude or negatively affect system capabilities. Today’s systems typically have numerous enhancing functions that improve performance but are not critical, and the software developers have no way to discern the difference between a critical system and an enhancing one without employing FMECA. In addition to identifying those non-essential functions, cyber vulnerability analyses need to be conducted on these non-essential systems as they are a prime target for cyber-attack. Hackers attempt to find the path of least resistance to affect a system's operations, and this path is often through non-essential functions similar to the hacker going through the in-flight entertainment system to access the 737 engine controls.

Integrating the Tools, Techniques, and Analyses

All of the tools, techniques, and analyses presented in this research must integrate with the existing Defense Acquisition System, or they will not be useful for DoD PMs. Figure 2 depicts how they integrate in the development of the system from the user requirements towards the Critical Design review (CDR).

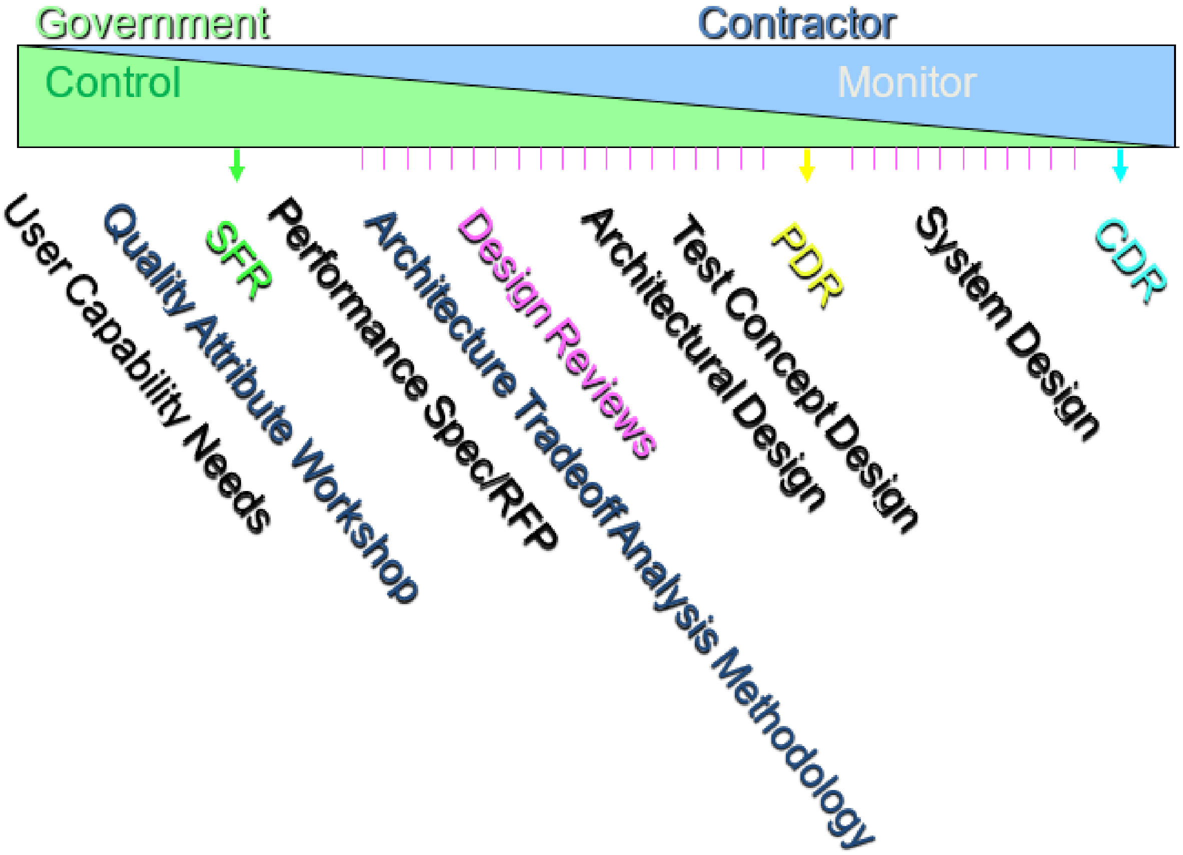


Figure 2. **Tools, Techniques, and Analyses Integration Into Design Activities**

Figure 2 shows how the government (green) controls the early functions and then monitors the contractor (blue) efforts in the system design process. The QAW is part of the requirements development process and assists in the requirements translation into the performance specification for the Request for Proposal (RFP). The requirements are formally set in the Systems Engineering Process (SEP) at the System Functional Review (SFR) depicted in the figure. The ATAM becomes an integral process within the Design Review (purple) iterative process and serves as the government's input during the early design reviews. The ATAM assists with the contractor's architectural design process and the

ATAM test case development contributes to the development of both the contractor and the government testing concept development. With the proper focus on cyber performance, the system will be designed from the initiation with cyber at the forefront and the testing concept will provide validation of cyber vulnerability mitigation efforts. The purposeful design with traceable cyber elements and associated testing validation fully supports the tenets of the RMF depicted in Figure 3.

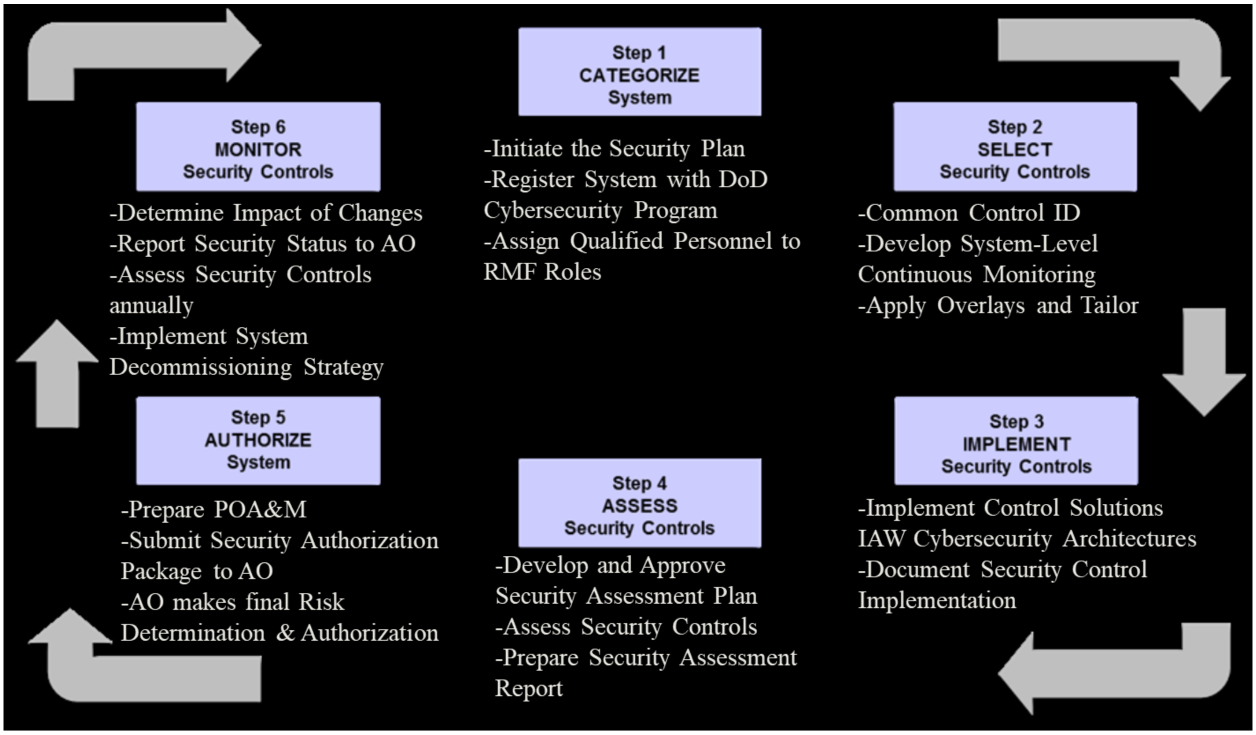

Step 1
CATEGORIZE
System
-Initiate the Security Plan
-Register System with DoD Cybersecurity Program
-Assign Qualified Personnel to RMF Roles
Step 2
SELECT
Security Controls
-Common Control ID
-Develop System-Level Continuous Monitoring
-Apply Overlays and Tailor
Step 3
IMPLEMENT
Security Controls
-Implement Control Solutions IAW Cybersecurity Architectures
-Document Security Control Implementation
Step 4
ASSESS
Security Controls
-Develop and Approve Security Assessment Plan
-Assess Security Controls
-Prepare Security Assessment Report
Step 5
AUTHORIZE
System
-Prepare POA&M
-Submit Security Authorization Package to AO
-AO makes final Risk Determination & Authorization
Step 6
MONITOR
Security Controls
-Determine Impact of Changes
-Report Security Status to AO
-Assess Security Controls annually
-Implement System Decommissioning Strategy

Figure 3. **The DoD Risk Management Framework (RMF)**
(DoD, 2015, p. 4)

As depicted in Figure 3, the RMF is a continuous and iterative process to continually assess the cyber security aspects of a system. Following the RMF steps, it is clear that the addition of the tools, techniques, and analyses to the DAS provides a method to conduct the RMF assessment from concept to implementation. In step 5, “Authorize,” the system’s Plan of Action and Mitigation (POA&M) is submitted as part of the security authorization package to the authorizing official (AO), who makes the final cyber risk determination and authorization for the system.

Conclusions and Recommendations

The explosive growth of cyber-attack types and variations, especially with the advent of AI-generated attack modes, makes it nearly impossible to be reactive to new threats. To avoid reacting to every new cyber threat, PMs must thoroughly understand and manage their system’s cyber vulnerabilities. To achieve this, PMs must exercise much more control over their system’s architectural design than is currently anticipated with the Defense Acquisition System (DAS), which cedes much of the design control to the contractor.

System components that are particularly vulnerable to cyber threats must be designated as Configuration Items and the design and configuration management must be completely controlled by the government. These include any components that have communications ability, system sensors, virtually all system software, and any other components deemed to have cyber vulnerabilities. This has significant implications for using commercial components and software, or even reuse of software. To understand the system's cyber vulnerabilities, the system component architecture, including software, must be thoroughly understood and controlled. To achieve this in software, the total code architecture must be known and most commercial software will not allow that level of access, as it is considered proprietary. Commercial software data rights are typically unobtainable. Even if data rights could be obtained, the level of engineering effort required to understand the inherent cyber vulnerabilities may exceed the effort to actually build the software from scratch, reducing or eliminating the acquisition cost advantage.

The tools, techniques, and analyses presented in this research augment the DAS to help the PM gain visibility and control of the system design, which is necessary to gain a complete inventory of system cyber vulnerabilities. Effective application of these tools, techniques, and analyses helps inform the Risk Management Framework (RMF) cyber vulnerability assessment techniques, which is what the RMF authorizing official needs to make the final risk assessment and authorization for the system under consideration.

MUIRS (Maintainability, Upgradeability, Interoperability, Reliability, and Safety/Security) Analyses

The MUIRS analyses was designed to help compensate for the DoD requirements generation shortcomings, which too often omit or vaguely articulate performance in each one of these areas even though they are important to the warfighter and impact the system Total Ownership Cost (TOC) significantly. The MUIRS elements also include areas where cyber vulnerabilities may exist and these analyses will likely help identify areas for cyber vigilance.

QAW (Software Engineering Institute's Quality Attribute Workshop)

While the QAW is a software-oriented technique, it is highly effective in fully developing a system's requirements, including the requirements for cyber performance. It was designed to help identify a more complete inventory of requirements, including derived and implied requirements not well identified or defined from the JCIDS and RFP Performance Specification processes. Including the MUIRS analyses as part of the QAW, the resulting requirements inventory is more complete and helps identify potential cyber vulnerabilities to be managed and mitigated.

ATAM (Software Engineering Institute's Architectural Trade-Off Analysis Methodology^{sm})

Another software-oriented methodology, ATAM is designed to more fully develop the system operational and lifecycle context needed to produce a far superior architectural design, especially in software. ATAM is most effective when it integrates the QAW and MUIRS processes. It features user-produced scenarios providing operational context detail not typically provided in the government-generated Operational Mode Summary/Mission Profile (OMS/MP), but absolutely essential for the software engineer to design an effective software system. The scenario development is extremely valuable in identifying potential areas for cyber vigilance including use cases, growth cases that can identify future interoperability needs and technology refreshment events, and exploratory scenarios that identify user expectations while the system is under attack, including cyber-attack. The exploratory scenarios include system FMECA (Failure Modes and Effects Criticality Analysis) scenarios, which can identify both critical and non-critical systems and functions that may reveal potential cyber vulnerabilities.

FMECA (Failure Modes and Effects Criticality Analysis)

The “failure modes” analyses include failure modes induced by adversaries through attacks or intrusion into the systems, so includes cyber warfare as part of the analyses. The “effects” analyses may help in developing cyber vulnerability mitigation strategies. The “criticality” analyses are designed to separate the critical from the non-critical failure modes, but may also help find non-critical systems that pose substantial cyber vulnerabilities as adversaries seek non-critical systems for cyber-attack as they typically have weaker or non-existent cyber defense mechanisms.

Summary

Integrating these tools, techniques, and analyses into the defense acquisition system provides the PM a far superior ability to identify, control, and mitigate the system cyber vulnerabilities in a cost-effective manner. Managing the system vulnerabilities is a better strategy than reacting to the constantly emerging cyber threats and fully supports the DoD Risk Management Framework tenets.

References

Barbacci, M., Ellison, R., Lattanze, A., Stafford, J., Weinstock, C., & Wood, W. (2003, August). *Quality attribute workshops (QAWs)* (3rd ed.) (CMU/SEI-2003-TR-016). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Blanchard, B. S. (2004). *Logistics engineering and management* (6th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Capaccio, A. (2019, January) The Pentagon’s cybersecurity is falling behind. Retrieved from https://www.bloomberg.com/news/articles/2019-01-28/pentagon-s-cybersecurity-found-unable-to-stay-ahead-of-attackers

DoD. (2015, September). *DoD program manager’s guidebook for integrating the cybersecurity Risk Management Framework (RMF) into the system acquisition lifecycle*. Washington, DC: Author.

Kazman, R., Klein, M., & Clements, P. (2000, August). *ATAM^{SM}: Method for architecture evaluation* (CMU/SEI-2000-TR-004). Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute.

Martini, P. (2016, September). Cybersecurity is threatening America’s military supremacy. Retrieved from https://techcrunch.com/2016/09/21/cybersecurity-is-threatening-americas-military-supremacy/

Naegle, B. R. (2006, September). *Developing software requirements supporting open architecture performance goals in critical DoD system-of-systems* (NPS-AM-06-035). Monterey, CA: Naval Postgraduate School.

Naegle, B. R. (2014, December). *Gaining control and predictability of software-intensive systems development and sustainment* (NPS-AM-14-194). Monterey, CA: Naval Postgraduate School.

Naegle, B. R., & Petross, D. (2007, September). *Software architecture: Managing design for achieving warfighter capability* (NPS-AM-07-104). Monterey, CA: Naval Postgraduate School.

Organization of Public Broadcasters (OPB). (n.d.). Activate your cell phone’s FM chip. Retrieved March 1, 2019, from https://www.opb.org/about/connect/mobilefm/

Pellerin, C. (2017, May). Cybercom: Pace of cyberattacks have consequences for military, nation. Retrieved from DoD website: https://dod.defense.gov/News/Article/Article/1192583/cybercom-pace-of-cyberattacks-have-consequences-for-military-nation/

Tarrant-Cornish, T. (2017, August 17). Chinese hackers ‘built back door hack into software to spy on Britain’s top businesses.’ *Express Online News.* Retrieved from https://www.express.co.uk/news/world/842200/China-hackers-cyber-spying-attack-UK-business

Ware, D. G. (2015, May). Hacker took control of United flight and flew jet sideways, FBI affidavit says. United Press International. Retrieved from https://www.upi.com/Top_News/US/2015/05/16/Hacker-took-control-of-United-flight-and-flew-jet-sideways-FBI-affidavit-says/2421431804961/

Panel 3. Observations on Category Management—Early Successes, Challenges, and Opportunities for Research

Wednesday, May 9, 2019	
10:30 a.m. – 11:45 a.m.	**Chair: Richard Lombardi,** Deputy Under Secretary of the Air Force, Management (SAF/MG) **Discussants:** **Major General Cameron Holt, USAF,** Deputy Assistant Secretary for Contracting, Office of the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics **Mr. Stuart Hazlett,** Deputy Assistant Secretary of the Army (Procurement) **Ms. Lorna B. Estep,** Executive Director, Air Force Installation & Mission Support Center

Richard Lombardi—Mr. Lombardi is the Deputy Under Secretary of the Air Force, Management and Deputy Chief Management Officer, Office of the Under Secretary of the Air Force, Arlington, Virginia. Mr. Lombardi exercises the Under Secretary's Chief Management Officer responsibility for improving the effectiveness and efficiency of Air Force business operations. In that role, he advises Air Force senior leadership on establishing strategic performance goals and managing Air Force-wide cross-functional activities to meet those goals. He also serves as the Air Force's Director of Business Transformation, overseeing implementation of continuous process improvement initiatives Air Force wide.

Mr. Lombardi was born in Lowell, Massachusetts. He entered the Air Force in 1980 after receiving his commission as a distinguished graduate of the ROTC program at the University of Lowell, Massachusetts. Mr. Lombardi has been assigned to acquisition management positions at the Air Armament Center, Electronic Systems Center and Headquarters Air Force Systems Command, as well as acquisition logistics positions at the San Antonio Air Logistics Center. He retired from the Air Force as a colonel in July 2004 and entered federal civil service. He was appointed to the Senior Executive Service in 2005. Prior to assuming his current position, Mr. Lombardi served as Special Assistant for the Invisible Combat Wounds Initiative, Office of the Under Secretary of the Air Force, Washington, D.C.

Major General Cameron Holt, USAF— Maj. Gen. Cameron G. Holt is the Deputy Assistant Secretary for Contracting, Office of the Assistant Secretary of the Air Force for Acquisition, Technology and Logistics, Washington, D.C. He is responsible for all aspects of contracting relating to the acquisition of weapon systems, logistics, and operational support for the Air Force and provides contingency contracting support to the geographic combatant commanders. He leads a highly skilled staff of mission-focused business leaders supporting warfighters through $825 billion of Space, Global Power/Reach and Information Dominance programs. He also oversees the training, organizing and equipping of a workforce of some 8,000 contracting professionals who execute programs worth more than $65 billion annually.

Prior to this assignment, General Holt served as the Commander, Air Force Installation Contracting Agency, Office of the Assistant Secretary of the Air Force for Acquisition, Wright-

Patterson Air Force Base, Ohio. He led an over 700 personnel agency with a total contract portfolio of $55 billion. In this capacity, he directed enterprise-wide installation strategic sourcing efforts for the Air Force and oversaw $9.1 billion in annual obligations for mission and installation requirements.

General Holt received his commission through the ROTC at the University of Georgia in 1990. He has experience in the full spectrum of acquisition and contract management across four major commands, Headquarters U.S. Air Force, U.S. Air Forces Central Command and the Joint Staff. General Holt is a joint qualified officer with multiple deployments in support of Operation Enduring Freedom.

Mr. Stuart Hazlett—Stuart A. Hazlett assumed the position of Director of Contracting, United States Army Corps of Engineers (USACE) in January 2012. He serves as the delegated Head of the Contracting Activity by the Chief of Engineers and directly exercises authority over three Principal Assistants Responsible for Contracting, ten

Regional Contracting Chiefs, and four Center Contracting Chiefs. Mr. Hazlett has overall responsibility for managing the contracting activity in support of USACE that has presence in more than 30 countries supporting Military Programs, Civil Works, Real Estate, and Research and Development. Under his cognizance, Mr. Hazlett executes approximately 62,000 contracting actions with obligations annually of $25 billion.

Before taking his current position, Mr Hazlett served as the Deputy Director of Program Acquisition & Strategic Sourcing (PASS) for Defense Procurement and Acquisition Policy (DPAP). In this role he served as a senior advisor to the Director of DPAP, Director of Defense Pricing, and the Under Secretary of Defense for Acquisitions, Technology, and Logistics in the Office of the Secretary of Defense. Mr. Hazlett supported Defense Acquisition Boards, Defense Acquisition Executive Summaries, and various Overarching Integrated Product Teams for major defense acquisition and special interest programs. He promoted the development of sound program acquisition strategies and fostered continuous and effective communication within the acquisition community to ensure effective application of associated statute and policy.

Prior to the aforementioned position he served as the Deputy Director of Strategic Sourcing for the Director of DPAP. In collaboration with the DoD components, his directorate conducted spend analyses and facilitated business solutions that permitted the department to achieve best value in strategically sourcing goods and services within a $370B spend across the department. He served as the Chair of the Strategic Sourcing Directors Board (SSDB) and as the department’s representative to the Federal Chief Acquisition Officer Council Strategic Sourcing Working Group.

Ms. Lorna B. Estep—Lorna B. Estep, a member of the Senior Executive Service, is the Executive Director, Air Force Installation and Mission Support Center, Joint Base San Antonio-Lackland, Texas. She directs the management of human and financial resources in a single Air Force enterprise, utilizing a $6.4 billion annual budget to provide installation and mission support capabilities to 77 Air Force installations, 10 major commands and two direct reporting units. The center also serves as the parent organization for 10 detachments co- located at each major command and six primary subordinate units including the Air Force Civil Engineer Center, Air Force Financial Management Center of Expertise, Air Force Financial Services Center, Air Force Installation Contracting Agency, Air Force Security Forces Center and Air Force Services Activity.

Ms. Estep started her career as a Navy logistics management intern. She has directed the Joint Center for Flexible Computer Integrated Manufacturing, was the first program manager for Rapid Acquisition of Manufactured Parts, and has served as Technical Director of Information Technology Initiatives at the Naval Supply Systems Command. In these positions she has developed logistics programs for the Department of Defense, implemented one of the first integrated and agile data-driven manufacturing systems, and directed the development of complex technical data systems for the Navy.

As the Director of Joint Logistics Systems Center, Ms. Estep carried out the duties of a commanding officer for a major subordinate command. In addition, she acted as the Logistics Community Manager, an emerging organization to coordinate and implement the revised Defense Department logistics strategy for achieving Joint Vision 2010 through modern information techniques and processes. She has also served as Chief Information Officer for the Naval Sea Systems Command in Arlington, Va.; Executive Director of Headquarters Materiel Systems Group at Wright-Patterson AFB; Deputy Director for Logistics Readiness at the Pentagon; Executive Director, Air Force Global Logistics Support Center; and Deputy Director, Logistics, for Air Force Material Command. Prior to her current assignment she was the Director of Resource Integration, Deputy Chief of Staff for Logistics, Engineering and Force Protection, Headquarters U.S. Air Force, Washington, D.C.

Panel 4. Our Most Important Asset: Acquisition Workforce

Wednesday, May 8, 2019	
10:30 a.m. – 11:45 a.m.	**Chair: Rene' Thomas-Rizzo,** Director, Resources, Personnel and Data, Office of the Under Secretary of Defense for Acquisition and Sustainment ***A Study of Financial and Non-Financial Incentives for Civilian and Military Program Managers for Major Defense Acquisition Programs*** Dave Hunter and Dave Tate, Institute for Defense Analyses ***Is the Army Acquisition Workforce Surfing the Federal Retirement Wave to a Soft Landing?*** Daniel Stimpson, Mark Nickituk, and Miesha Purcell, Army Director, Acquisition Career Management ***Enhancing Professional and Technical Excellence: Analysis of Navy Contract Management Competency Models*** Rene Rendon, Naval Postgraduate School

A Study of Financial and Non-Financial Incentives for Civilian and Military Program Managers for Major Defense Acquisition Programs

David E. Hunter—joined IDA in 1997 shortly after earning a PhD in operations research from the State University of New York at Buffalo, and is currently the Deputy Director of the Cost Analysis and Research Division (CARD). During his 20-plus years at IDA, he has led numerous high-profile projects. Dr. Hunter received IDA's Andrew J. Goodpaster Award for Excellence in Research in 2010. He is a graduate of the Harvard Kennedy School program for Senior Executives in National and International Security and a fellow in the MIT Seminar XXI program. [dhunter@ida.org]

David M. Tate—joined the research staff of IDA's CARD Division in 2000. Prior to that, he was an Assistant Professor of Industrial Engineering at the University of Pittsburgh and the Senior Operations Research Analyst (Telecom) for Decision-Science Applications, Inc. At IDA, he has worked on a wide variety of resource analysis and quantitative modeling projects related to national security. These include an independent cost estimate of Future Combat Systems development costs, investigation of apparent inequities in Veterans' Disability Benefit adjudications, and modeling and optimization of resource-constrained acquisition portfolios. Dr. Tate holds bachelor's degrees in philosophy and mathematical sciences from the Johns Hopkins University, and MS and PhD degrees in operations research from Cornell University. [dtate@ida.org]

Abstract

The Institute for Defense Analyses (IDA) was asked to conduct a comprehensive study of financial and non-financial incentives for civilian and military program managers (PMs) for major defense acquisition programs in response to the requirement in Section 841(b)(1) of the National Defense Authorization Act for Fiscal Year 2018. In this study, the IDA team reviewed relevant previous research, interviewed government and industry personnel, analyzed data, and identified and assessed incentives to recruit, retain, and reward Department of Defense PMs.

Introduction

The Institute for Defense Analyses (IDA) was asked to conduct a congressionally-mandated comprehensive study of financial and non-financial incentives for civilian and military program managers (PMs) for major defense acquisition programs (MDAPs). Specifically, IDA was asked to examine and assess additional pay options for PMs to provide incentives to senior civilian employees and military officers to accept and remain in PM roles, a financial incentive structure to reward PMs for delivering capabilities within budget and on time, and a comparison between financial and non-financial incentive structures for PMs in the Department of Defense (DoD) and an appropriate comparison group of private industry companies.

IDA took a multi-faceted approach to this assessment, including conducting numerous interviews, reviewing the extensive collection of existing literature, and collecting and analyzing data on past PMs. A summary of our approach and our main findings are described later. A more complete description of our methodology and findings can be found in Hunter et al. (2018).

Literature Review

An extensive body of published literature addresses DoD materiel acquisition, including the duties, authority, responsibilities, and performance incentives of DoD PMs. Schwartz, Francis, and O'Connor (2016) report that 150 major studies on acquisition reform have been published since the end of World War II. The most influential of these have articulated that improvement of the acquisition workforce is the key to acquisition reform. Most of the official literature that describes the DoD acquisition system makes little distinction between a civilian and a military PM (Office of the Under Secretary of Defense for Acquisition, Technology, & Logistics [OUSD(AT&L)], 2017), other than that some PM positions are designated as military only (United States Army Acquisition Support Center, 2014, p. 19).

Career Overview

A DoD PM generally "manages" multiple interrelated projects. Fox (2011, p. 194), among others, points out that the duties of DoD managers of large acquisition programs are not those classically associated with the term "manager" because the DoD does not develop or produce its weapon systems in-house; rather, the development and production work is contracted through prime contractors. The principal functions of PMs and their staffs are planning, contracting, monitoring, controlling, and evaluating the schedule, cost, and technical performance of the contractors and government agencies that provide services and support.

The Congress, as a matter of policy, has mandated that

> appropriate career paths for civilian and military personnel who wish to pursue careers in acquisition are identified in terms of the education, training, experience, and assignments necessary for career progression of civilians and members of the armed forces to the most senior acquisition positions. (10 U.S.C. § 1722(a), 2019)

Military personnel are not given exclusive access to senior acquisition positions, including PM positions. The Congress has provided,

> The Secretary shall establish a policy permitting a particular acquisition position to be specified as available only to members of the armed forces if a determination is made, under criteria specified in the policy, that a member of the armed forces is required for that position by law, is essential for performance of the duties of the position, or is necessary for another compelling reason. (10 U.S.C. § 1722(b)(2)(A), 2019)

Each Military Department is required "to establish policies and issue guidance to ensure the proper development, assignment, and employment of members of the armed forces in the acquisition field" (10 U.S.C. § 1722a(a), n.d.).

While there are important differences in how the Military Departments have chosen to implement these directives, the passage of the Defense Acquisition Workforce Improvement Act (DAWIA; Pub. L. No. 101-510, 1990) and subsequent amendments has ensured that the basic structure of military acquisition workforce careers is the same across the DoD. Military officers elect to enter the acquisition workforce after six to seven years of service, joining an acquisition-related career field. Program management is one such career field. After completing certain mandatory training requirements and time in acquisition-related positions, they are eligible to join the Acquisition Corps, typically at a rank of O-4 (GAO, 2018).[1] While in theory these officers compete for promotion with the general pool of officers, in practice all three departments monitor the proportion of officers promoted to ensure that promotion rates within the Acquisition Corps are comparable to those in operational command tracks. Promotion reviews occur every three years; promoted officers are transferred to new duties commensurate with their new ranks. Officers passed over for promotion in two successive reviews are retired from the Service.

The Congress has pushed back in recent years against having all military acquisition career paths feature a one-time permanent transition into the acquisition workforce. Section 842 of the National Defense Acquisition Act for Fiscal Year (FY) 2016 added the language quoted previously that distinguishes single-track from dual-track acquisition careers. The House report on this bill characterized this section as "reinstituting a dual-tracking system of primary and functional secondary career fields" (H. Rept. No. 114-201, 2015, to accompany H. R. 1735). The Senate report said,

> This provision is designed to increase the attractiveness of acquisition functions to skilled military officers and enlisted personnel and would: (1) provide for credit for joint duty assignments for acquisition related assignments in order to broaden the promotion preference and career opportunities of military acquisition professionals; (2) provide for an enhanced dual track career path in combat arms and a functional secondary career in acquisition to more closely align military operational requirements and acquisition; (3) include business and commercial training as joint professional military education; and (4) require an annual report to Congress on promotion rates for officers in acquisition positions. (S. Rept. No. 114-49, 2015, to accompany S. 1376)

While it is not explicitly stated in the statute or the conference reports, it seems likely that the intent of the Congress was to re-establish career paths that move back and forth multiple times between acquisition and combat arms assignments. This is not current practice within any of the Military Departments.

Civilians in all Services are managed and promoted within civilian workforce management systems common across the DoD. The vast majority of these civilians fall within the General Schedule for federal employees or the Acquisition Workforce Demonstration Project (AcqDemo), which is discussed in more detail in Section 0. DAWIA sets requirements for certification, including education and years of experience, for both civilians and uniformed personnel occupying PM positions. It is DoD policy that anyone occupying a key leadership position, as an Acquisition Category (ACAT) I or IA PM, must be Level III-certified in their respective functional area, and they must have eight years of acquisition experience or equivalent demonstrated proficiency. ACAT II PMs and deputy PMs must have six years of acquisition experience.

[1] The GAO notes that the Air Force typically identifies future Acquisition Corps officers earlier in their careers and tailors their early career assignments toward that goal in ways that the Army and Navy do not.

Data Analyses on the Tenures of MDAP Program Managers

To observe historical tenure of MDAP PMs, we obtained data from December 1997 to December 2017 on 705 PMs of 202 MDAPs from the Selected Acquisition Reports (SARs) stored in the Defense Acquisition Management Information Retrieval (DAMIR) System.[2] Specifically, each SAR lists the name, contact information, and assignment date of the PM at the time the SAR was produced. The prefix for each name identifies either the rank, for military PMs, or the title (e.g., Mr., Ms.), for civilian PMs, enabling us to identify each PM's personnel type (military or civilian). From the assignment dates, we were able to construct a timeline of PMs for each program. Because the SARs are only submitted once each year, it is possible that the timelines we constructed missed a few PMs who may have very briefly served in between the end of one SAR and the assignment date of the PM who is listed on the subsequent SAR. In these cases, the timelines will overstate the tenures of the PMs immediately preceding the "missing" PMs.[3]

Table 1 shows the distribution of MDAPs and PMs across the Services from the DAMIR data. We observe a total of 705 PMs for 202 past and present MDAPs. Seventeen percent of these PMs are civilians. Of the Services, the Air Force currently has the highest percentage of civilian PMs (36%), although the Navy has the highest number of civilian PMs over the whole sample (24%). About half of PMs for (the relatively small universe of) DoD-wide programs have been civilians.

Table 1. Summary of MDAPs and PMs by Service from December 1997 to December 2017

	Current Programs			**All Programs (12/1997 to 12/2017)**		
	No. of Programs	**No. of Military PMs**	**No. of Civilian PMs**	**No. of Programs**	**No. of Military PMs**	**No. of Civilian PMs**
Army	17	15	2	64	166	23
Navy	40	34	6	63	183	58
Air Force	28	18	10	71	227	29
DoD-wide	2	1	1	4	9	10
Total	**87**	**68**	**19**	**202**	**585**	**120**

Table 1 shows the distribution of tenures for completed MDAP PM positions by personnel type. The tenure distributions are very similar between military and civilian PMs. Half of the 82 civilians PMs served less than 2.92 years, with 75% serving 3.92 years or less. Half of the 390 military PMs served for less than 3.04 years, with 75% less

[2] SARs are annual comprehensive status reports that each MDAP is required to submit to the Congress.

[3] For example, suppose there are three PMs: Amy, Bill, and Carl. The December 2000 SAR reports Amy as the PM with an effective date of January 1, 2000, and the December 2001 SAR reports Carl as the PM with an effective date of June 1, 2001. If Bill served as PM from January 1 to May 31, 2001, his tenure is not reported on any SAR, and our constructed timelines incorrectly assume that Amy served as PM from January 2000 until Carl's start date in June 2001.

than 3.95 years. Not surprisingly given the structured promotion process, military PM tenures tend to cluster around the 2-, 3-, and 4-year marks.

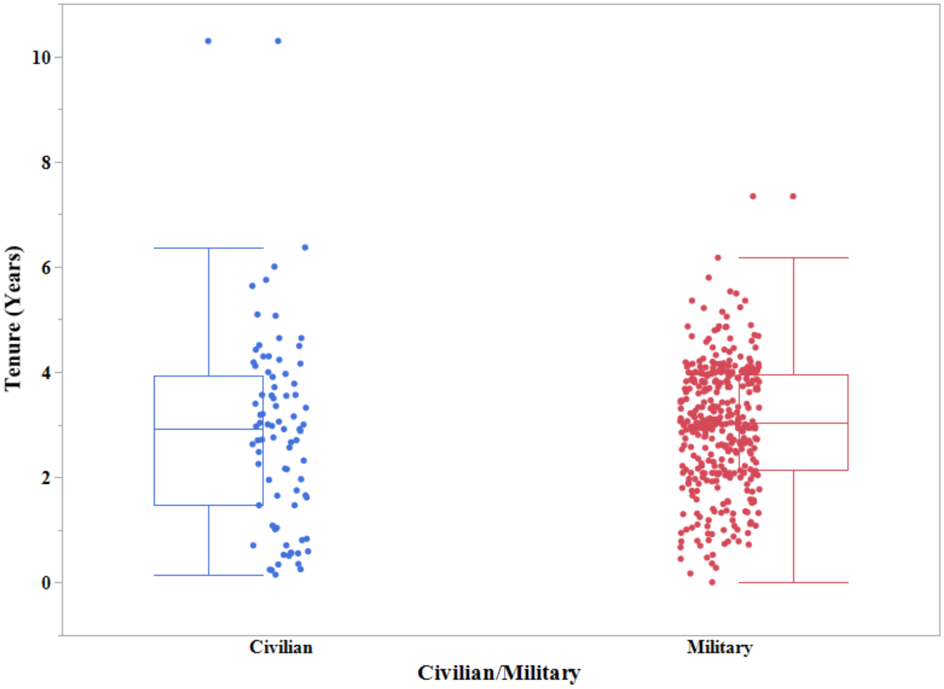
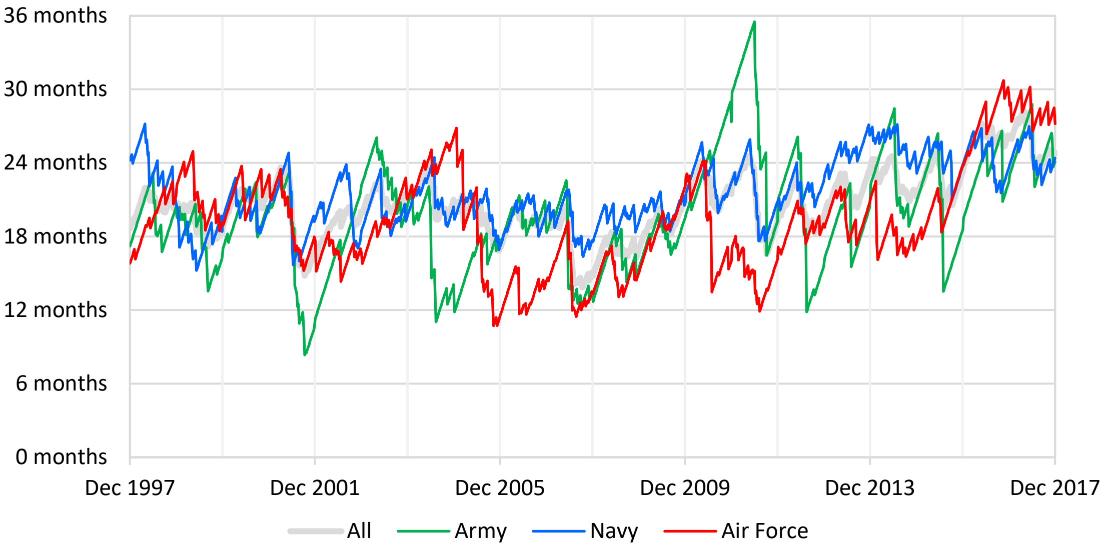


Figure 1. **Distribution of Completed Tenures for Civilian and Military MDAP PMs**

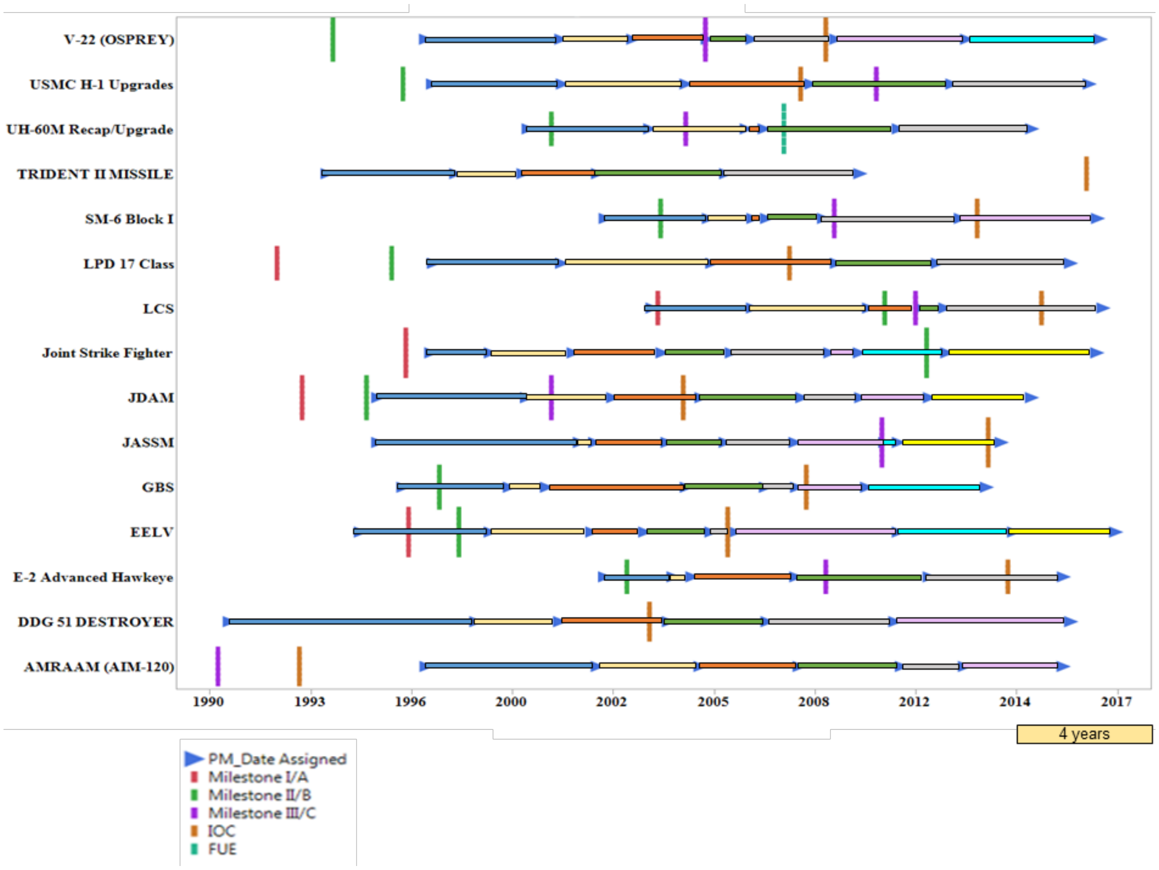
Figure 1 shows the average time in position broken out by Service. Overall, the average experience of MDAP PMs has grown from about 18 months in December 1997 to about two years in December 2017. The Services' averages show the same general trend.



Note. Each line represents the averages of time in position for every MDAP PM within a Service at each moment in time.

Figure 2. **Average Time in Position of MDAP PMs Over Time, by Service**

The SARs also list past and projected milestone dates for each program. Since the milestone dates can slip over time, we collect data on completed milestones (i.e., milestones that occurred before the SAR date). **Error! Reference source not found.** shows how these milestone dates compare to changes in PMs for 15 current programs.[4] Visually, it appears that while most PMs within four years of a milestone complete that milestone, many PM transitions are unrelated to upcoming milestones. For example, there were at least three PM transitions in the four years leading up to Milestone C of the Standard Missile-6 (SM-6 Block I) program.



Note. Only milestones that occurred since 1990 are shown. Also, when the same program milestone took place more than once, only the latest one is presented.

Figure 3. **PM Tenures Compared Against Milestones for Selected MDAPs**

[4] Specifically, these are the 15 current programs that are either ACAT I or IA, have at least six PM transitions, and have most of the program milestones.

Summary of Findings

Additional Pay Options to Provide Incentives to DoD PMs

Senior Civilian Employees

Government civilians, like their military counterparts, are motivated by challenging work, a sense of accomplishment, and career-enhancing opportunities. Financial rewards have been found to be low on the priority list for public employees. However, our analysis showed that average compensation for DoD civilian PMs is significantly lower than for similar military PMs and those in private industry. Establishing a separate, higher pay scale for civilians who have chosen the Program Management career track could incentivize more and higher quality civilians to pursue such careers. Some efforts in this direction have already been made. AcqDemo, introduced in 1999, established an alternative personnel system for qualifying civilian acquisition workforce employees. Expanding AcqDemo further and/or making it permanent would almost certainly enhance future recruiting and retention.

One of the largest non-financial changes that could be made to encourage future civilian PMs is Component Acquisition Executive slating of more MDAP PM positions to civilians and a gradual lessening of the perception that civilians do not have much of a chance of being selected. Presently, civilians may be unmotivated to pursue a career leading to an MDAP PM position if they see little chance of ever being selected and see no future career path in the rare event that they are.

The ability to have more control over planning one’s career path would be another important non-financial incentive for civilians in program management and acquisition. Currently, qualified civilians may shy away from applying for MDAP PM positions due to uncertainty about the location and responsibility of their subsequent assignments.

Military Officers

Given existing constraints on the military pay system, the primary financial incentive available to the uniformed services is special and incentive pay. The literature on financial incentives for military personnel is mixed, but the consensus has been that financial incentives are less effective in the public sector—including in the military—than in private industry.

Currently, the strongest incentives for military officers are related to the promotion process. Failure to be promoted not only reduces current salary and eventual retirement pension, but also can curtail a career due to the “up-or-out” provisions of the Defense Officer Personnel Management Act (DOPMA). As a result, factors that affect potential for promotion have a strong influence on choices made by military officers. The current DOPMA mandates might be considered major disincentives and, as noted in several previous studies, eliminating or modifying both up-or-out and mandatory retirement at 30 years of service could help the Department recruit and retain more skilled and experienced PMs. These changes would also enable more flexible career paths, allowing for fewer (but longer) assignments over the course of a career.

As with civilians, developing better-defined career tracks for PMs could be an important non-financial incentive for attracting military officers. One particular alternative would be to establish a more self-contained professional system for recruiting military officers into the acquisition field, similar to that used for the medical field. This would more closely mirror best practices from industry.

A Financial Incentive Structure to Reward Program Managers

It has been suggested that merit-based incentives (rewards) are the best mechanism for motivating PMs to manage their programs effectively and efficiently. As an example, PMs who meet certain cost and schedule targets could be offered spot bonuses—or even commendations and/or medals. High-performing PMs could be rewarded with more control over their next assignments, especially if the DOPMA up-or-out policy and mandatory retirement do not interfere. While the Congress is seeking ways to reward PMs who deliver capabilities within budget and on time, recognizing the challenge of accurately measuring PM performance is particularly important because of the dangers of establishing rewards for performance that do not ultimately align with the organization’s mission.

Performance-based rewards can have significant unintended consequences when they are applied in the wrong context. Research has shown repeatedly that poorly specified reward systems can create perverse incentives—incentivizing workers to focus on obtaining the rewards rather than on achieving organizational objectives. A reward system focused on cost and schedule may encourage short-term optimization at the expense of the long-run success of the program. For example, PMs may be incentivized to accept greatly increased future sustainment cost and obsolescence risk in order to avoid missing milestones or having to report cost growth.

A Comparison With Incentives in Private Industry

Although sharing the same title, PMs in government do not have the duties historically associated with the title of “manager” because the DoD does not develop or produce its weapon systems in-house. Rather, the development and production work is contracted through prime contractors. The principal functions of the government PM and staff are planning, contracting, monitoring, controlling, and evaluating the schedule, cost, and technical performance of contractors and the government agencies that provide services and support.

Past research finds that public sector managers are often attracted to their work by different factors than private sector managers. Extrinsic motivation factors (e.g., salary, pension plans, and career advancement) have significantly greater potential for motivating private managers, while intrinsic rewards (e.g., challenging and interesting work, job responsibility, advancement/promotion in a hierarchical organization, family-friendly policies, commitment to the public interest, a desire to serve others, self-sacrifice, and recognition) have higher potential for motivating public managers. These differences suggest that different systems of rewards and incentives than those found in the private sector might be best suited to recruit and retain quality government PMs.

For-profit companies have the option to motivate their PMs to achieve organizational objectives by rewarding them with a portion of company profits. Industry PMs who carefully manage successful programs and quickly shut down poor programs that are destined to fail can share in the higher profits their actions bring their companies. The industry PMs who fail may lose their jobs. In contrast, there are no company profits to share with DoD PMs, and acquisition personnel are not subject to the threat of dismissal from the Service on failure as their industry counterparts are. As a result, success tends to be measured in terms of cost and schedule and avoiding cancellation.

Concluding Thoughts

We have focused our efforts in this research on the consideration of the pros and cons of potential incentives to recruit, retain, and reward PMs. We find, as with previous research, only weak evidence that financial incentives would have any impact on the actual tenures of PMs. Moreover, past research finds little support for the implicit assumption that increased PM tenure would have a significantly positive effect on program outcomes such as cost and schedule.

If the real goal is to improve program outcomes, there are likely to be more effective mechanisms than simply increasing the tenure of PMs. For example, the DoD could pursue an acquisition centered around “smart buyers.” Credible “smart buyers”—such as highly experienced senior program executive officers (PEOs) and PMs—could provide the counterweight that helps to overcome the institutional and political pressures to overpromise at the outset of programs. They further could help to enforce realism in executing programs in the face of contractor optimism. A career progression model, with strong rewards for successful careers, could create the “smart buyer” culture needed to properly develop and incentivize PMs and PEOs to serve as counterweights to political and institutional pressures. Because of their experience, and the career incentive structure, senior acquisition personnel would be positioned to make proper decisions based upon real experience.

Industry experience has shown that another important best practice for maintaining a healthy portfolio is to identify and quickly terminate programs that are unlikely to succeed. Creating policies and a culture that supports failing quickly would be a substantial challenge, but the payoff to the overall outcomes of the entire MDAP portfolio would be considerable.

References

10 U.S.C. § 1722(a) (2019).

10 U.S.C. § 1722a(a) (n.d.).

10 U.S.C. § 1722(b)(2)(A) (2019).

Defense Acquisition Workforce Improvement Act, Pub. L. No. 101-510 (1990).

Fox, J. R. (2011). Defense acquisition reform, 1960–2009: An elusive goal. Washington, DC: Center of Military History, United States Army.

GAO. (2018). Defense acquisition workforce: Opportunities exist to improve practices for developing program managers (GAO-18-217). Washington, DC: Author. Retrieved from https://www.gao.gov/assets/700/690094.pdf

H. Rept. No. 114-201 (2015), to accompany H. R. 1735.

Hunter, D. E., Breen, M., Cummins, M. G., Diehl, R. P., Huff, N. M., Oh, E., … Tate, D. M. (2018). A study of financial and non-financial incentives for civilian and military program managers for major defense acquisition systems (IDA Paper P-9245). Alexandria, VA: Institute for Defense Analyses.

Office of the Under Secretary of Defense for Acquisition, Technology, & Logistics (OUSD[AT&L]). (2013). Key leadership positions and qualification criteria [Memorandum]. Washington, DC: Author.

Office of the Under Secretary of Defense for Acquisition, Technology, & Logistics (OUSD[AT&L]). (2017). Operation of the defense acquisition system: Incorporating change 3 (DoD Instruction 5000.02).

S. Rept. No. 114-49 (2015), to accompany S. 1376.

Schwartz, M., Francis, K. A., & O’Connor, C. V. (2016). The Department of Defense acquisition workforce: Background, analysis, and questions for Congress (CRS Report R44578). Washington, DC: Congressional Research Service. Retrieved from https://fas.org/sgp/crs/natsec/R44578.pdf

United States Army Acquisition Support Center. (2014). 2014 handbook: Civilian project/product manager.

Is the Army Acquisition Workforce Surfing the Federal Retirement Wave to a Soft Landing?

Daniel E. Stimpson—PhD, is an Operations Research Systems Analyst (ORSA) at the U.S. Army Director of Acquisition Career Management (DACM) Office and Associate Professor at George Mason University (GMU). He holds a master's degree and a PhD in operations research from the Naval Postgraduate School and George Mason University, respectively. Before joining the Army DACM office, he retired from the Marine Corps after 24 years of both enlisted and officer service. He has also been an ORSA with the Center for Naval Analyses, the GMU research faculty, the Joint Improvised Explosive Device Defeat Organization (JIEDDO), and Headquarters Marine Corps (HQMC).

Marko J. Nikituk—is the Army Acquisition Workforce Analysis and Planning Branch Chief in the Army DACM Office. He is an Army Acquisition Corps member with 15 years of acquisition experience. He is Level III Certified in Program Management and Information Technology Management. He earned a master's degree in information technology management from the Naval Postgraduate School, and a bachelor's degree in electrical engineering from the U.S. Military Academy. He is a retired Infantryman, with duty in the Program Executive Office Enterprise Information Systems, the Army DACM Office, the Army CIO/G6, Army Programming Analysis & Evaluation (PA&E), and the Deputy Under Secretary of the Army for Business Transformation.

Miesha L. Purcell—is an Operations Research Analyst (ORSA) at the Army DACM Office. She has worked with and maintained the data in the Career Acquisition Personnel Position Management Information System (CAPPMIS) for more than eight years. She holds a bachelor's degree in computer science from Columbus State University and a master's degree in information technology systems from George Washington University. Before joining the Army DACM Office, she worked as a software engineer at ArgonST.

Abstract

For several years, attrition in the defense acquisition workforce has been a serious and persistent concern among stakeholders inside and outside of government, especially attrition related to baby boomer retirement. The primary concern relates to the risk of losing critical skills and experience required to maintain and improve enterprise effectiveness. The Army Director of Acquisition Career Management (DACM) defines retirement "brain drain" as generational retirement with the potential to create a talent vacuum.

While change is inevitable and institutional transitions usually involve turbulence and friction, to date the Army Acquisition Workforce (AAW) has maintained its base of experienced workforce members and made steady progress improving workforce balance despite the rising retirement wave.

This paper presents highlights of recently completed comprehensive data analysis that provides a view of recent trends within the AAW's 14 career fields. We also demonstrate the importance of proper problem-framing in developing an accurate understanding of the current state of the AAW and what dynamics led to it.

Introduction

For more than a decade, stakeholders inside and outside of government raised concerns about potential severe negative effects related to generational retirement of baby boomers (Defense Acquisition University, 2007; Gates, et al., 2008; Hogan, Lockley, & Thompson, 2012; Professional Services Council, 2016; Gates et al., 2018). A primary concern relates to the loss of the critical skills and experience required to maintain and improve enterprise as a high volume of seasoned employees exit the workforce. To the extent this occurs, the Army Director of Acquisition Career Management (DACM) defines retirement "brain drain" as generational retirement with the potential to create a talent vacuum (Techopedia.com, n.d.).

Baby boomers, born between 1946 and 1964, are now between ages 54 and 74. With federal retirement eligibility beginning at age 55 (depending on a person's federal years of service [YoS]), today nearly 100% of baby-boomer federal employees are within the retirement eligibility window.

Effectively managing the current retirement situation for the AAW's demographically diverse civilian and military workforce is a critical function of Army DACM Office efforts under its Human Capital Strategic Plan (HCSP; U.S. Army, n.d.). This requires a comprehensive understanding of recent accession and separation patterns that led to the current state of the AAW and implications these suggest for the path ahead.

U.S. Population Distribution

As Figure 1 shows, since the last baby boomers were born in 1964, the demographics of the United States changed considerably. The left side of the figure shows the U.S. birthrate for the two decades before 1964 grew the base of the U.S. population pyramid,[1] resulting in the characteristic shape of an expanding population. In contrast, the 2018 population pyramid (middle chart) has nearly vertical edges tapering to a slightly narrower base. This is characteristic of a decreasing birth rate, which in a closed society would indicate a shrinking population. But, in fact the U.S. population is increasing due to immigration. Finally, the right side of Figure 1 shows the U.S. Census Bureau projection for the U.S. population to continue growing through the next 10 years, maintaining its population pyramid shape consistent with low birthrates, long life expectancies, and continued immigration (Colby & Ortman, 2014; Colby & Ortman, 2015).

[1] A population pyramid is the combination of vertically oriented, back-to-back male and female histograms of the population counted according to age.

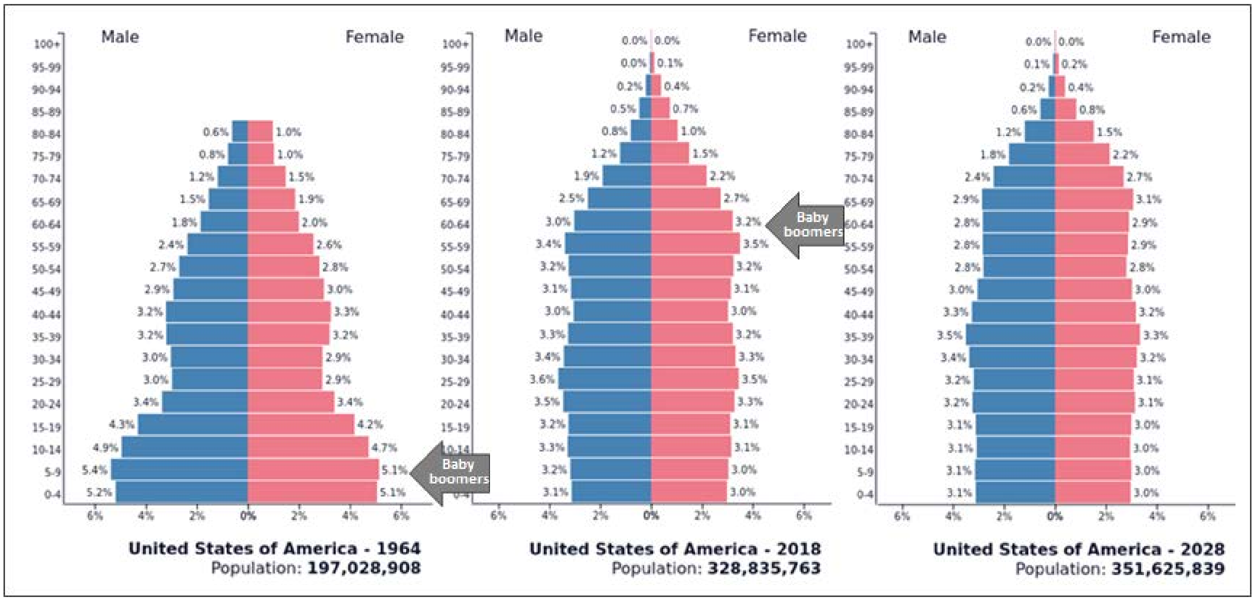


Figure 1. **Population Pyramids for United States of America (Population Pyramid, n.d.)**[2]

Importantly, the diagrams in Figure 1 show no significant age distribution imbalance in the current or projected U.S. population, which is the primary context for AAW recruiting and retention. So while personal choices related to accepting employment and worker mobility are complex phenomena involving factors such as overall job satisfaction, perceived opportunities, personal skills, employer demand, geography, and timing, U.S. population age distributions cannot be blamed for AAW age imbalances that may currently exist or develop in the foreseeable future.

Army DACM's Human Capital Strategic Plan (HCSP)

The 2002 President's Management Agenda recognized the potential for a significant institutional brain drain as the result of baby-boomer retirement. The agenda also recognized the need for better recruiting, retention, and reward programs for federal workers. Toward this end, the Department of Defense (DoD) generated a department-wide strategic human capital plan followed by the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L])[3] strategic human capital plan for the Defense Acquisition Workforce (Gates, et al., 2008). The current DoD Acquisition Workforce Strategic Plan—FY 2016–FY 2021 (AWSP) is the latest in the series of updates since 2002.

The DoD's AWSP reports that overall, Acquisition Workforce (AWF) gains exceeded losses from FY 2008 through FY 2015 with significant improvement in the pending

[2] Age is on the vertical axis.

[3] On February 1, 2018, the fiscal year 2017 National Defense Authorization Act eliminated the USD(AT&L) position to re-establish the position of Under Secretary of Defense for Research and Engineering (USD[R&E]) and create the new position of Under Secretary of Defense for Acquisition and Sustainment (USD[A&S]).

retirements “bathtub,”[4] better posturing the workforce for the high level of retirements the plan expects. Further, the AWSP expresses concern about the potential for losing critical AWF experience and capacity as the current workforce ages and retires (DoD, 2016).

The AWSP also sets forth four strategic goals, with Goal 2 being to “shape and develop the AWF to meet current and future mission area demands” (DoD, 2016). Within this effort, the Army DACM developed a Human Capital Strategic Plan (HCSP) which establishes five of its own goals to institutionalize the human capital planning process and develop the next generation of Army acquisition leaders. The first of these is to “shape the Army acquisition workforce to achieve current and future acquisition requirements” which fits squarely under the AWSP’s Goal 2.

Goal 1 of the Army DACM’s HCSP encompasses five broad categories:

- Labor supply
- Labor demand
- Recruiting the workforce
- Managing workforce separation
- Steering labor supply to fit labor demand

Thus, this goal is intentionally forward-looking with the intent of setting the conditions for mission success with proactive policies and planning. This requires reliable projections of future workforce demographics and dynamics, based on well understood cause-and-effect relationships. To develop these, the DACM Office works to gain accurate understandings of past workforce dynamics and current trends across the AAW as a foundation for its ongoing predictive modeling effort.

Data and Definitions

The Army DACM’s Career Acquisition Personnel and Position Management Information System[5] (CAPPMIS) maintains the data used in this study. CAPPMIS includes direct feeds from the Defense Civilian Personnel Data System (DCPDS) and provides, among other information, every employee’s age, duration of federal employment, duration of acquisition experience, acquisition certification status, command assignment, and geographic location.

For this analysis, we compared annual individual civilian personnel records on September 30 each year from 2012 through 2018[6]. From these we categorize each employee as a “join,” “stay,” or “loss” according to the annual snapshots in which they appear. If an employee appears in two consecutive records, we define them as “stayed” in the AAW for the fiscal year (FY) spanned by the two data snapshots. If an employee record appears in a prior year snapshot, but not in a later one, we counted them as a “loss.” Likewise, if an employee appears in a later snapshot, but not in the previous one, we

[4] “Bathtub” is a term used in the acquisition community to describe imbalances in workforce experience, i.e., a severe shortage of procurement professionals with between 5 and 15 years of experience (Acquisition Advisory Panel, 2007).

[5] CAPPMIS provides quarterly feeds to Defense Manpower Data System (DMDC).

[6] All data are according to CAPPMIS on March 31, 2019.

counted them as a “join.” This methodology means migrations within the AAW (changes of employment command or location) are not considered.[7]

From these data, five primary measures are calculated as of the beginning of each FY:[8]

- Age: Calculated using the Date of Birth field in DCPDS
- YoS: *Years of service* are determined according to the Service Computation Date in DCPDS
- YRE: *Years until retirement eligible* are calculated according to FERS retirement eligibility criteria based on the minimum retirement age, and years of service (YoS) for individuals with 100% earned benefit[9] (Office of Personnel Management, 2019). For year-over-year comparison we round to an integer value, so YRE = 0 means an individual became retirement eligible (RE) within the FY spanned by applicable data snapshots. If YRE < 0, then an individual is RE for the entire FY. While YRE > 0 means an individual is not RE at any time in the applicable FY.
- YAE: *Years of acquisition experience* counts the total number of years of work experience an individual has within the AAW in any Acquisition Career Field (ACF). Individuals self-report their acquisition experience in other agencies, military, or contractor roles.
- RE: We categorize joins, stays, and losses as retirement eligible if they become retirement eligible at any time during a given FY. Therefore, it is important to note the number of RE reported in this analysis is an annual total and values are higher than those commonly reported in single point-in-time (snapshot) counts. We emphasize this difference throughout this paper with the use of the word “annual” to describe the findings (e.g., we discuss annual losses and annual RE gains).

One challenge of AAW trend analysis is the constantly changing size of the workforce Figure 2 shows the scale of these changes which vary by Acquisition Career Field. Year-over-year variations result from the changes in service acquisition and program requirements, employee choices, and career field recoding. Recoding occurs when positions are either created or eliminated according to mission and command priorities. The most significant AAW recoding since FY13 is the large increase of Facility Engineers between FY17 and 18 which occurred due to U.S. Army functional leader policy decisions (shown in Shown in Figure 2).

[7] Stay = Continuation, Loss = Attrition, and Gain = Accession.

[8] In order to use the most recent value recorded, all data are standardized to the beginning of the applicable FY as follows: Joins and Stays data are read from the later year data snapshot and data field entries are converted the beginning of the FY (e.g., Age(FY14) = Age(FY15)-1). Losses are recorded in the previous year snapshot only, so their values are read from the prior FY snapshot without adjustment.

[9] While retirement eligibility depends on each individual’s retirement plan, more than 96% of the AAW is currently under FERS.

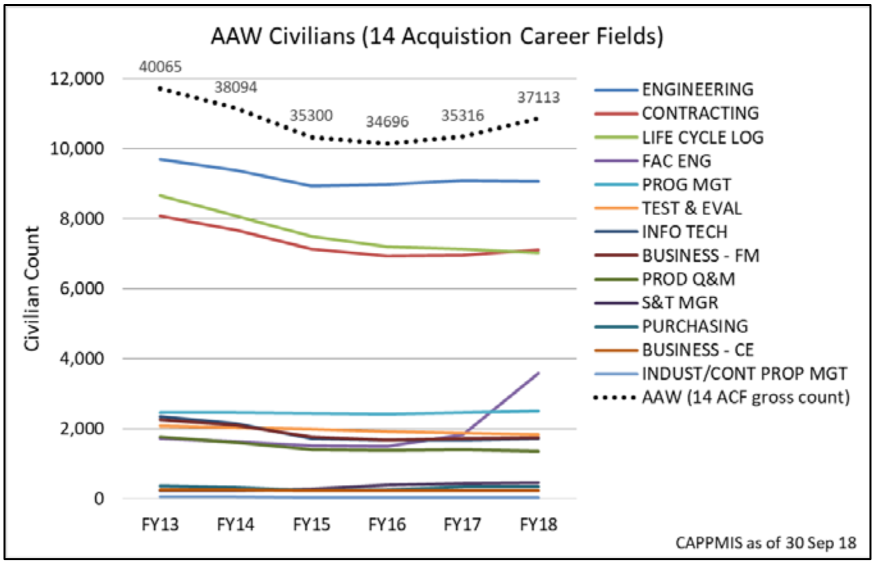


Figure 2. **Count of AAW Civilian Personnel in Each Army ACF (at Beginning of FY)**

The Bathtub Effect

The term *bathtub effect* describes the phenomenon of simultaneously having an excessive number of senior acquisition professionals, many in and near retirement eligibility, and an underrepresentation of mid-level employees to succeed them when they retire (Acquisition Advisory Panel, 2007; Hogan et al., 2012).

For more than 20 years, an ongoing concern of senior leadership is the bathtub effect phenomenon among the civilian AW. In 2000, the USDs for AT&L and Personnel and Readiness (P&R) stated that “after 11 consecutive years of downsizing, we face serious imbalances in the skills and experience of our highly talented and specialized civilian workforce. Further, 50 percent will be eligible to retire by 2005. In some occupations, half of the current employees will be gone by 2006” (USD[AT&L]; USD[P&R], 2000). Because this condition has persisted, it has been repeatedly highlighted since.

For example, in 2005 the Defense Acquisition University (DAU) found that 76% of the AT&L workforce were baby boomers or older (Defense Acquisition University, 2007). Again in 2007, the Acquisition Advisory Panel reported to the U.S. Congress that

> During the 1990s, the federal AW was significantly reduced and hiring virtually ceased, creating what has been termed the Bathtub effect, a severe shortage of procurement professionals with between 5 and 15 years of experience. The impact of this shortage is likely to be felt more acutely soon, as half of the current workforce is eligible to retire in the next four years. (Acquisition Advisory Panel, 2007)

A 2009 RAND study concluded that the number of DoN retirement-eligible AW personnel would increase by 2012 and remain above average for at least seven years (Gates, 2009).

Thus, senior defense acquisition leaders maintained focus on filling the bathtub as a persistent theme by codifying it into strategy documents and addressing it in policy decisions.

Figure 3 shows the civilian AAW age and RE distributions at the beginning of both FY13 (dashed line) and FY18 (solid line). Comparing these distributions immediately highlights the importance of how we frame the RE situation. On the left-hand side is the “Age-frame” and on the right side is the “YRE-frame.” Each entails a very different perception of the state of the AAW. The age distribution is distinctly bimodal in both FY13 and FY18, with the FY18 mode near 55 years of age, i.e., the beginning of federal retirement eligibility. This peak indicates a significant “bow wave” as 29% of the “stay” population was at least 55 years of age in FY18. This view from the age-frame makes the potential for an AAW brain drain appear acute and critical.

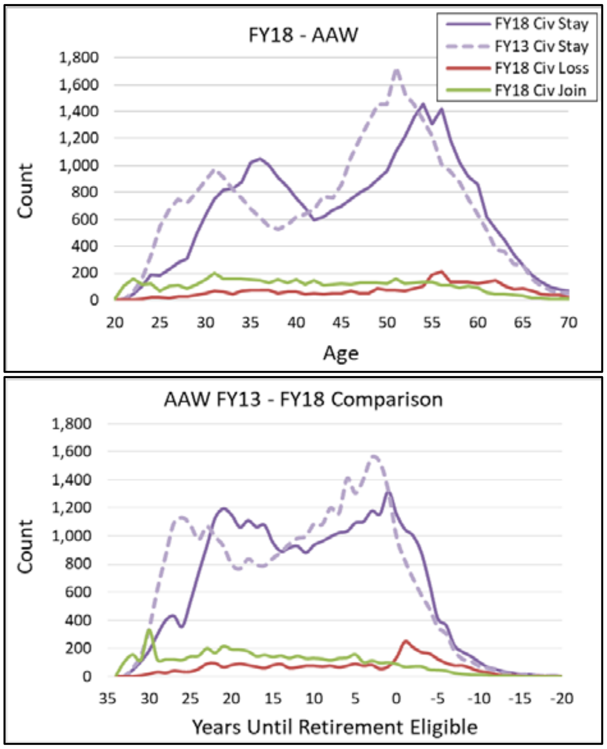


Figure 3. **AAW Civilian Employee Age and Retirement Eligibility Distribution Comparisons (September 30, 2012, and September 30, 2018)**

The right-hand side of Figure 3 shows the YRE distribution. Like the age distribution, the YRE distribution is distinctly bimodal, but the leading peak height is nearly equal to the trailing peak. And the bathtub (5 ≤ YRE ≤ 15) is not nearly as deep. When comparing FY13 to FY18, we see that there has been a leveling of the employee distribution while the “bathtub” has been filling. Thus, unlike what we see in the age-frame, this view shows workforce balance has improved over the six-year period.

Figure 4 shows the development of these changes over time as a series of six YRE distributions for AAW joins and losses. This reveals an important dynamic. First, in FY13 and FY14 the red lines (losses) exceeded the green lines (joins), across most of the YRE distribution. From FY16 through FY18 this pattern inverted with joins exceeding losses across the whole not-RE population (i.e., YRE < 0). This difference increased each year after FY15, providing positive feedback to intentional DACM workforce shaping efforts ranging from improved employee engagement to targeted hiring and retention efforts, as well as position recoding. Further, these charts show results are both wide-spread and sustained.

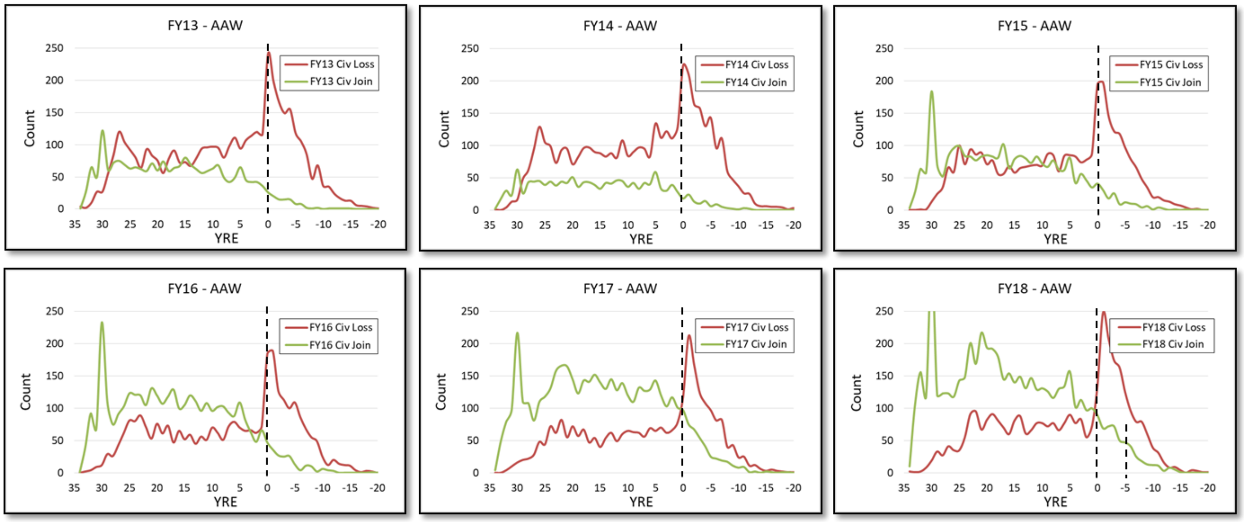


Figure 4. **Historical Joins and Losses by YRE, FY13 Through FY18**

Figure 5 aggregates the data displayed in Figure 4. This representation reveals several other important outcomes of the recent AAW join and loss patterns. First, total annual AAW losses (the solid red line) were lower in FY18 than in FY13, even after increasing from FY17 to FY18. As shown, declining losses among employees who were not-RE drove down the decrease in total annual losses. These were the majority of losses in all years (66% in FY13 and 59% in FY18). This is a decrease in annual not-RE losses of 665 (from 2660 in FY13 to 1995 in FY18) against a generally consistent number of annual RE losses which increased by 50 (or 3.7%) from FY13 to FY18 (1356 and 1406 annual losses respectively).

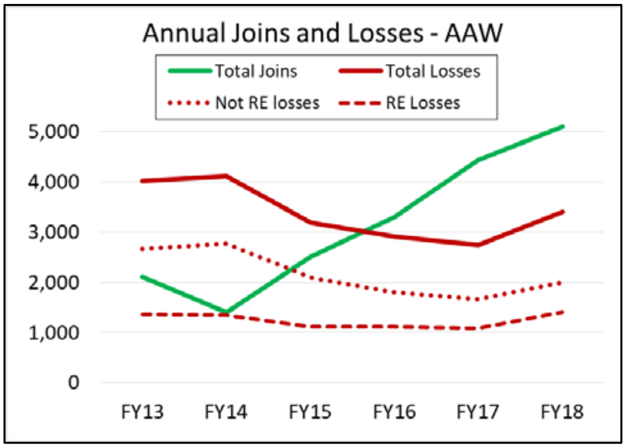


Figure 5. **AAW Join and Loss Rates**

Figure 5 also shows annual losses increased from FY17 to FY18 in both RE and not-RE categories (see the two dashed lines). It is too early to know whether this change indicates normal variation or a trend reversal, so we will continue to collect data and assess this. The latter case appears likely for reasons we will discuss in the next section. Finally, the dramatic change in number of joins (green line in Figure 5) is clearly evident as annual joins increased from 2115 in FY13 (about 50% less than total annual losses) to 5104 in FY18 (about 50% more than total annual losses).

These figures illustrate the importance of not focusing solely on the retiring workforce, as the majority of attrition occurs among those not in the RE window.

Consequently, successful recruiting and retention in the early career population are proving effective workforce shaping and preservation drivers for combating the bathtub effect and more than compensating for FY17 and FY18 retirement flows.

AAW Retirement Rate

The green bars in Figure 6 show how the annual number of RE employees remained essentially unchanged FY13–FY15, but then began increasing from 6521 during FY15 to 7910 during FY18. As a percentage, those RE increased at about 1% per year from 16.1% of the AAW during FY13 to 21.3% during FY18 (this is shown by the green line). Meanwhile, the red bars show that annual losses from this group (RE losses) remained consistent during the same period. In fact, despite the increasing RE population during FY16 and FY17, RE losses continued decreasing until FY17, when the trend reversed, bringing FY18 RE losses back to about the FY13 level. Further, as a percentage of the RE population (red line), these losses decreased from 23.1% in FY13 to 18.8% in FY18.

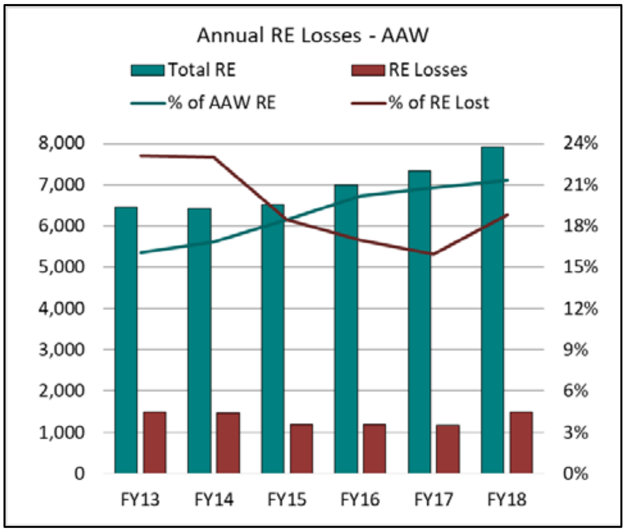


Figure 6. **AAW Retirement Eligible Population Trends**

The combined effect of these two trends suggests that retirement “pressure” is building in the civilian AAW population as the number retirement eligible has been increasing, while the number in this group actually leaving the workforce has not. This is why we expect the reversal from decreasing to increasing RE-losses between FY17 and FY18 is not likely attributable to normal variation, but will continue through FY19 and for as long as the RE population remains elevated.

These RE employee counts simply tell us who is eligible to retire according to the federal criteria, but they don’t tell us anything about who is retiring and what intellectual capital and expertise is leaving with them. While sheer numbers always matter, it is important to examine who is retiring, because job skills and relevant expertise are critical considerations for assessing potential retirement brain drain impacts.

AAW Retirement Brain Drain

Acquisition expertise is not something we can easily measure from the available data. But, all else being equal, increased job experience generally correlates with increased job expertise. Under this assumption, we use YAE as a proxy measure of expertise and intellectual capital as a gauge of brain drain. While this is a coarse measure, we find it helpful in evaluating the gross effects of workforce gains and losses on the overall AAW experience base. Additionally, since YAE is specific measure to the Army's acquisition enterprise, it is a proxy for the question at hand. We acknowledge that counting total years invested in the enterprise has the inherent weakness of only capturing acquisition experience broadly, without any specificity of expertise in any particular skillset, ACF, or acquisition program. But, just as comparing the age-frame to the YRE-frame provides important insights into the flow of retirees, we find comparing the YoS-frame to the YAE-frame helps us better understand likely impacts related to overall workforce expertise and brain drain.

The left-hand side of Figure 7 shows the stratified AAW distribution according to employee's federal YoS, with a breakout of those RE and near-RE[10] underneath. Juxtaposed, on the right-hand side, are charts showing the AAW distribution according to employee YAE, stratified by the same RE categories. According to YoS distribution on the left side, there is a clear retirement "bow wave" between 30 and 40 YoS (shown in in red and yellow). But, the YAE-frame on the right side reveals that the experience distribution of the pending AAW retirements is much more uniformly distributed (compare the second charts down on each side). Thus, the retirement wave is significantly less sharp when accounting for acquisition-specific experience leaving the AAW.

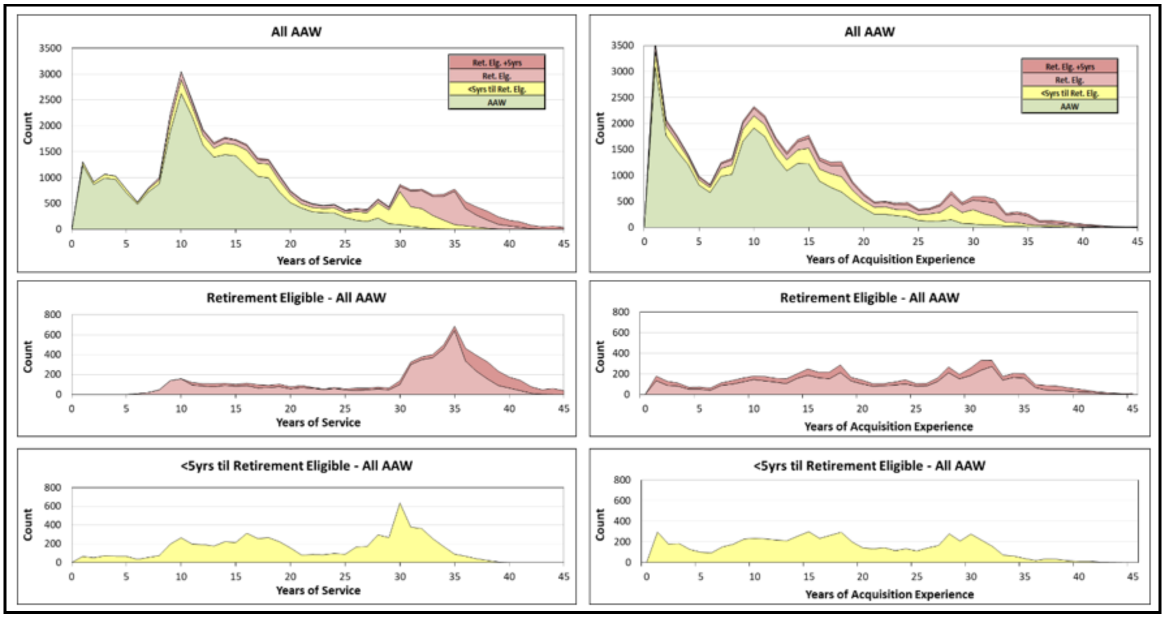


Figure 7. **Workforce Retirement Eligibility Distributions**

This comparison emphasizes the intuitive understanding that age does equal experience and federal workforce experience does not equal acquisition expertise. This is to say, not all workforce losses have equal impact on AAW intellectual capital. Each individual retirement, even with the same age and YoS, entails a unique skillset and experience for which the workforce must compensate when it is gone. Thus, since the Army hires many AAW employees in later career stages without previous acquisition experience, the total YAE they accrue are less than their age and YoS might suggest. When we measure this

[10] Near-RE are those within five years of RE.

directly, we see the total annual AAW expertise-loss is significantly smoother than the Age and YoS perspective implies.

Total AAW Acquisition Experience

We can measure experience gained and experience lost in the AAW by summing the total YAE. As such, each person who joins or leaves the AAW carries with them some number of YAE. Also, every member that remains in the AAW gains one YAE for every year they remain. From this we can make a simple calculation. For example, if the AAW has 39,000 civilian members that remain, then total AAW YAEs increase by 39,000 during that year. Then, so long as the sum of these 39,000 YAE and the YAEs of those joining is greater than the YAE of those leaving the workforce, the workforce does not suffer any loss of acquisition experience, that is, brain drain.

In FY13, the AAW had 40,100 civilian employees and 443,800 total YAE. In FY18, there were fewer civilian employees, 37,100, but more total YAE, 471,600 years. The red and green bars in Figure 8 show the YAE for AAW joins and losses during these years, while the black line shows mean YAEs, which increased from 11.1 in FY13 to 12.7 in FY18. It is also important to note that the green bars in Figure 8 show that employees joining the AAW were not beginning with zero YAE. Rather, those joining had significant acquisition experience. During FY18, 30% of those joining the AAW had previous YAEs, averaging 7.1 years.

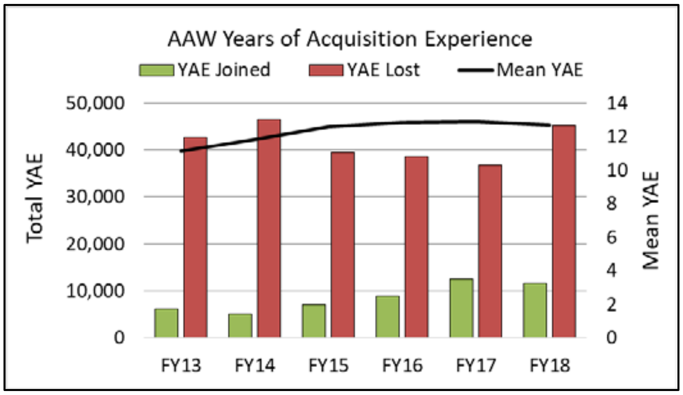


Figure 8. **Cumulative AAW Years of Acquisition Experience**

As an additional brain drain measure, we suggest 10 YAE is an important benchmark for the attainment of full job proficiency or acquisition expertise. Recent workforce survey results and academic research support this assumption. In 2017, MITRE reported workforce survey results from 250 DoD support personnel where 92% of respondents stated 10 or more years of work experience are required to become fully proficient in acquisition[11] (Murphy & Bouffard, 2017). This result is consistent with many human psychology findings that assert "experts are made, not born" and that skill mastery requires thousands of hours of specific, sustained practice and skill development (Ericsson, Krampe, & Clemens, 1993; Ericsson, Charness, & Felto, 2006; Ericsson, Prietula, & Cokely, 2007).

[11] 68% of respondents believed it takes 10 years, 18% believed it takes 15 years, 10% believed 20+ years.

Figure 9 displays the percentages of the annual join, stay, and loss populations with more 10 YAE. According to this measure, the percentage of "experts" staying in the AAW increased sharply between FY13 and FY18, from 41% to 52% respectively. Additionally, while the percentage of annual RE expert losses increased, the level remained consistently below the percentage staying. Further, this relationship remains across 11 of the AAWs 14 ACFs (which comprise 85% of the AAW).[12] These findings provide positive indication that the AAW is not suffering a damaging level of brain drain, even though considerable expertise is leaving every year.

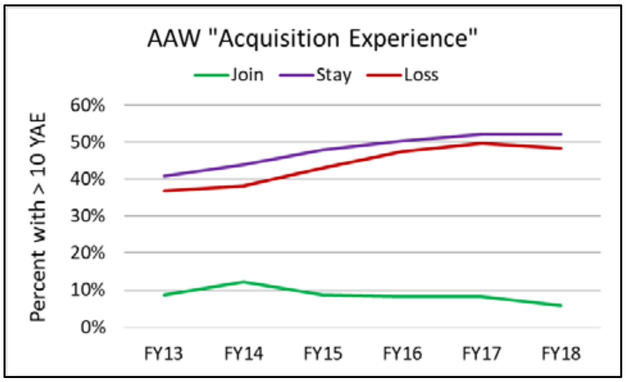


Figure 9. **Percent of AAW With More Than 10 YAE by Employee Category**

This outcome is expected in light of the increasing join rate relative to the loss rate shown in Figure 9 as these trends translate into increased employee tenure. It is also consistent with 2018 survey results where leaders across the federal acquisition enterprise reported generally increasing workforce skills (Professional Services Council, 2018).

Career Field Patterns and Trends

Because no career field or command is average, policy makers realize limited value from aggregated statistics that may miss important features within individual sub-populations. For example, Figure 10 is a side-by-side display of the primary measures presented in this paper to allow comparison of the Engineering and Contracting ACFs. Several important features are evident when assessing the brain drain potential of each.

[12] Facility Engineering (≈5000 members with ≈1700 newly recoded position during FY 18), S&T Manager (≈500 members), and Purchasing (≈300 members) are the exceptions.

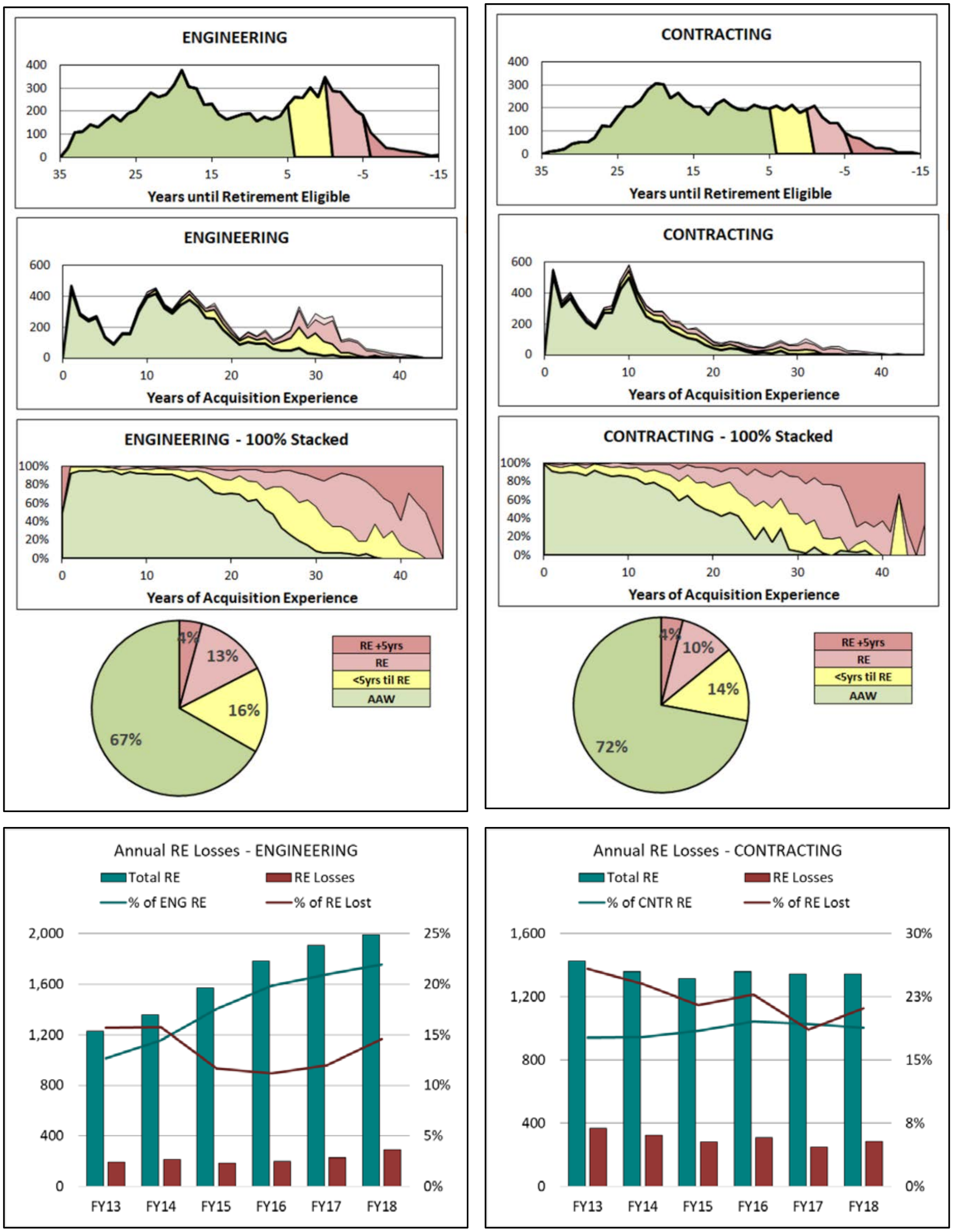


Figure 10. **AAW Engineering–Contracting Career Field Comparison**

We note the following indications of high brain drain potential in the Engineering ACF (left side of Figure 10):

1. Expected higher than average near-term retirement rate because:
    a. 34% of AAW engineers are RE or near-RE (pie chart)
    b. The RE Engineering population increased rapidly since FY13 (from 12.7% in FY13 to 21.9% in FY18, green line in bottom chart)
    c. The RE loss rate increased in FY17 and FY18 (from 11.1% in FY16 to 14.6% in FY18, red line in bottom chart)
2. Expected higher than average near-term RE experience loss because:
    a. The RE and near-RE population is heavily concentrated at YAE>25 (second chart from top)
    b. Underrepresentation of personnel with 5 and 20–25 YAE (second chart from top)
3. Engineering is the largest AAW career field (>9000 members) and 97% hold STEM degrees

For these and other reasons outside the scope of this paper, we assess Engineering as having the highest retirement brain drain potential of the AAW's 14 ACFs. The factors leading to Engineering's current condition developed over many years, but mainly occurred because of its historically low early and mid-career attrition. Accordingly, sustained lower than typical attrition, especially during early career phases, means retiring engineers currently have higher than average tenure than those retiring from other ACFs.

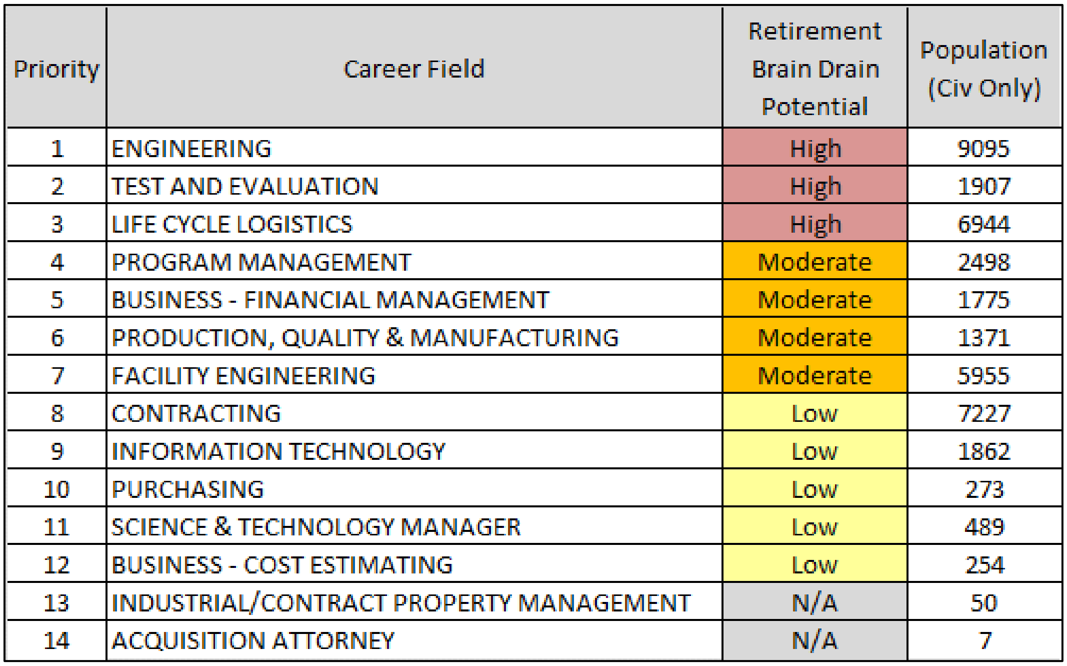
We note the following in the Contracting ACF (right side of Figure 10):

1. Expected moderate near-term retirement rate because:
    a. Favorable, unimodal YRE distribution with mode at 20 YRE (top chart)
    b. 29% of AAW contractors are RE or near-RE (pie chart)
    c. RE population has been stable since FY13 (changing from 17.7% in FY13 and FY14 to 18.8% in FY18, green line in bottom chart)
    d. The declining RE loss rate reversed in FY18, but remains down (from 25.8% in FY13 to 21.1% in FY18, red line in bottom chart)
2. Expected moderate near-term RE experience loss because the RE and near-RE population is spread across YAE (second chart from top)
3. Contracting is the second largest AAW career field (≈7000 members)

We assess Contracting as having a low retirement brain drain potential. The dynamics in this ACF are very different from those among engineers as they typically exhibit high early and mid-career attrition so that they have far fewer high tenure employees in the RE population.

Figure 11 displays a summary of our retirement brain drain assessment for all 14 AAW ACFs. The retirement brain drain potential is highest in the Engineering, Test & Evaluation, and Life Cycle Logistics career fields. Together, these career fields have about

18,000 employees who hold 60% of the science, technology, engineering, and mathematics (STEM) degrees[13] in the AAW.



Priority	Career Field	Retirement Brain Drain Potential	Population (Civ Only)
1	ENGINEERING	High	9095
2	TEST AND EVALUATION	High	1907
3	LIFE CYCLE LOGISTICS	High	6944
4	PROGRAM MANAGEMENT	Moderate	2498
5	BUSINESS - FINANCIAL MANAGEMENT	Moderate	1775
6	PRODUCTION, QUALITY & MANUFACTURING	Moderate	1371
7	FACILITY ENGINEERING	Moderate	5955
8	CONTRACTING	Low	7227
9	INFORMATION TECHNOLOGY	Low	1862
10	PURCHASING	Low	273
11	SCIENCE & TECHNOLOGY MANAGER	Low	489
12	BUSINESS - COST ESTIMATING	Low	254
13	INDUSTRIAL/CONTRACT PROPERTY MANAGEMENT	N/A	50
14	ACQUISITION ATTORNEY	N/A	7

Figure 11. **Retirement Brain Drain Potential Assessment Summary**[14]

Conclusion

This paper’s primary focus is understanding the character of the retiring population in order to understand implications related to brain drain from ongoing baby boomer retirement. This is only one of many important workforce management issues for policy makers to consider in crafting comprehensive strategies and policies. With nearly all AAW baby boomers now retirement-eligible, the often-threatened retirement wave is upon us. Even so, our assessment of the AAW is consistent with other results documenting the successful growing and balancing of the DoD AW (DAW) over the past decade (Gates et al., 2018).

We have shown that problem framing is critical to proper understanding of the retirement brain drain dynamic. Specifically, the YRE-frame and the YAE-frames provide more meaningful understanding of the brain drain potential across the workforce than the Age-frame and YoS-frame. Together these better capture the quantity and distribution of acquisition specific experience entering and leaving the workforce. Therefore, despite expected ongoing baby boomer retirements and increased near-term retirement rates, the AAW has been able to maintain its end strength, improve its workforce balance, and grow its

[13] STEM degrees are defined according to National Center for Education Statistics categories.

[14] Industrial/Contract Property Management and Acquisition Attorney career fields are too small to be assessed in aggregate.

experience base to enable critical Army DACM initiatives related to acquisition program success and leader succession.

Future Work

As the Army DACM continues executing the HCSP to shape the future rather than react to it, accurate readings of workforce dynamics are needed to enable continuous fine tuning. This will require increased measurement detail in areas such as acquisition expertise. In turn, efforts to improve acquisition expertise raise additional research questions. For example, DAW training certification rates have increased significantly in the last decade (USD[AT&L], 2016). The DACM is interested in better understanding the impact of this trend on mission effectiveness. Hence, we seek to assess research questions such as the following: How much does training translate into improved job performance? What training is most effective for increasing needed expertise? Answering cause-and-effect questions like these are critical to optimizing training resource allocation and driving improved mission effectiveness.

Other cause-and-effect relationships important to the Army DACM within the HCSP include measuring the effectiveness of communication channels on workforce engagement, measuring workforce engagement effects on worker retention, and measuring effects of workforce culture on leadership development.

Finally, we are pursuing increased specificity—for example, identifying and measuring precise recruiting and retention drivers of the best performing and highest potential employees, rather than the aggregated employee pool.

References

Acquisition Advisory Panel. (2007). *Report of the acquisition advisory panel to the office of federal procurement olicy and the United States Congress.* Washington, DC: U.S. Office of Management and Budget.

Colby, S. L., & Ortman, J. M. (2014). *The baby boom cohort in the United States: 2012 to 2060.* Washington, DC: U.S. Census Bureau. Retrieved from https://www.census.gov/content/dam/Census/library/publications/2014/demo/p25-1141.pdf

Colby, S. L., & Ortman, J. M. (2015). *Projections of the size and composition of the U.S. population: 2014 to 2060.* Washington, DC: U.S. Census Bureau. Retrieved from https://www.census.gov/content/dam/Census/library/publications/2015/demo/p25-1

Defense Acquisition University. (2007). *Defense acquisition structures and capabilities review.* Fort Belvoir, VA: Author.

DoD. (2016). *Acquisition workforce strategic plan FY2016–FY2021.* Washington, DC: Author.

Ericsson, A. K., Charness, N., & Felto, P. J. (2006). *The Cambridge handbook of expertise and expert performance* (Cambridge handbooks in psychology). Cambridge, England: Cambridge University Press.

Ericsson, A. K., Krampe, R. T., & Clemens, T.-R. (1993). The role of deliberate practice in the acquisition of expert performance. *Psychological Review, 100*(3), 363–406.

Ericsson, A. K., Prietula, M. J., & Cokely, E. T. (2007, July–August). The making of an expert. *Harvard Business Review, 85*(7/8), 114. Retrieved from https://hbr.org/2007/07/the-making-of-an-expert

Gates, S. M. (2009). *Shining a spotlight on the defense acquisition workforce—Again.* Santa Monica, CA: RAND Corporation.

Gates, S. M., Keating, E. G., Jewell, A., Daugherty, L., Tysinger, B., & Masi, R. (2008). *The defense acquisition workforce: An analysis of personnel trends relevant to policy, 1993–2006.* Santa Monica, CA: RAND Corporation. Retrieved from http://www.rand.org/pubs/technical_reports/TR572.html

Gates, S. M., Phillips, B., Powell, M. H., Roth, E., & Marks, J. S. (2018). *Analysis of the Department of Defense acquisition workforce: Update to methods and results through 2017.* Santa Monica, CA: RAND Corporation. Retrieved from http://www.rand.org/pubs/technical_reports/TR572.html

Hogan, B., Lockley, L., & Thompson, D. (2012). *Shaping the Navy's Acquisition Workforce* (MBA professional report). Monterey, CA: Naval Postgraduate School. Retrieved from https://apps.dtic.mil/docs/citations/ADA562791

Murphy, C., & Bouffard, A. (2017). Understanding defense acquisition workforce challenges. In *Proceedings of the 14th Annual Acquisition Research Symposium.* Monterey CA: Naval Postgraduate School. Retrieved from https://apps.dtic.mil/docs/citations/ADA562791

Office of Personnel Management. (2019, March 29). FERS information. Washington, DC: Author. Retrieved from https://www.opm.gov/retirement-services/fers-information/eligibility/

Population Pyramid. (n.d.). *Population pyramids of the world from 1950 to 2100.* Retrieved from https://www.populationpyramid.net/united-states-of-america

Professional Services Council. (2016). *Aligning for acquisition success: Overcoming obstacles to results.* Washington, DC: Grant Thornton. Retrieved from https://contractingacademy.gatech.edu/wp-content/uploads/2016/06/Acquisition-Policy-Survey-2016-1.pdf

Professional Services Council. (2018). *Aligning for acquisition success: Optimism amid adversity.* Washington, DC: Grant Thornton. Retrieved from https://www.grantthornton.com/-/media/content-page-files/public-sector/pdfs/surveys/2018/2018-PSC-Acquisition-Survey.ashx

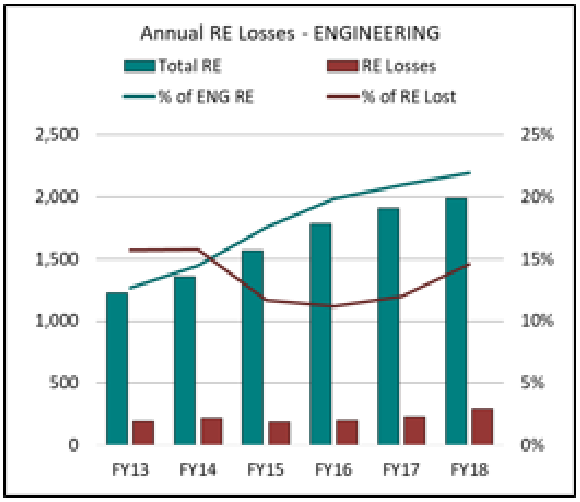
Techopedia.com. (n.d.). Brain drain. Retrieved from https://www.techopedia.com/definition/30085/retirement-brain-drain-rbd

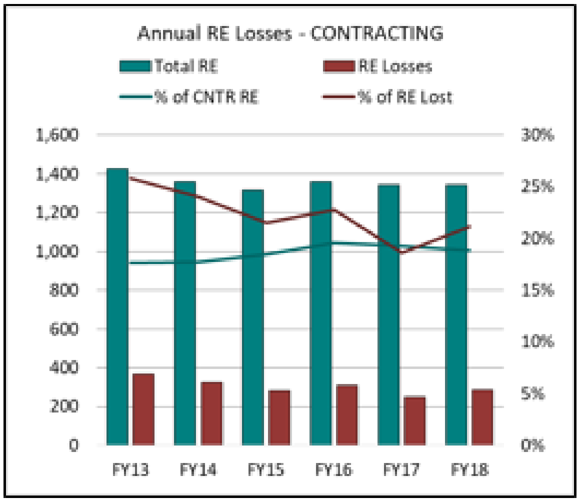
U.S. Army. (n.d.) *Army Acquisition Workforce Human Capital Strategic Plan (HCSP)*. Retrieved from https://asc.army.mil/web/hcsp

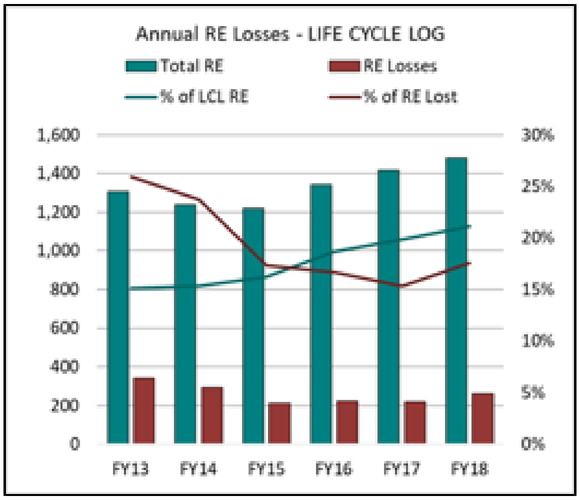
USD (Acquisition, Technology, & Logistics). (2016). *Performance of the defense acquisition system: 2016 annual report.* Washington, DC: DoD. Retrieved from https://apps.dtic.mil/docs/citations/AD1019605

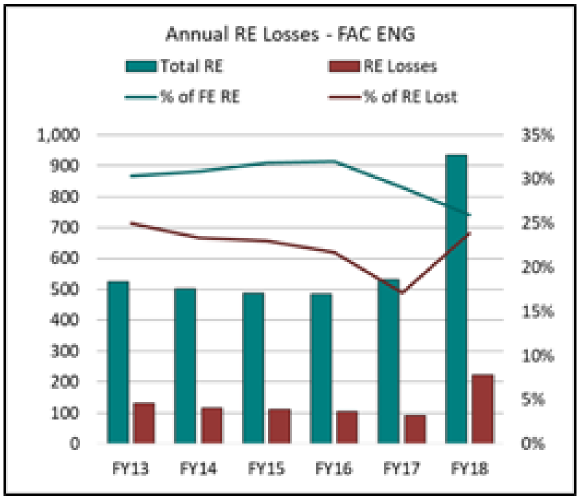
USD (Acquisition, Technology, & Logistics); USD (Personnel & Readiness). (2000). *Shaping the civilian acquisition workforce of the future.* Washington, DC: Office of the Secretary of Defense. Retrieved from http://www.acq.osd.mil/dpap/Docs/report1000.pdf

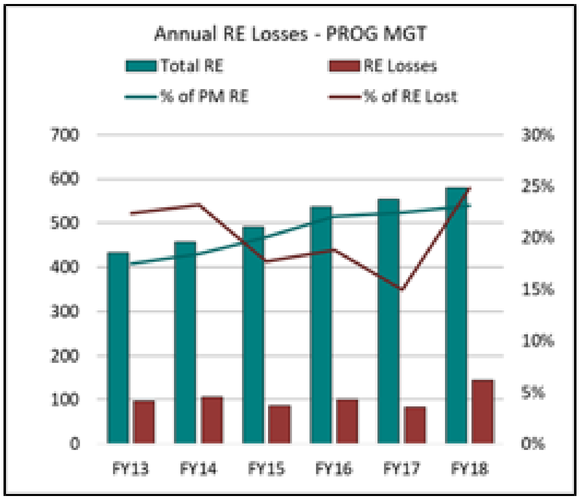
Appendix: Career Field Summary Charts

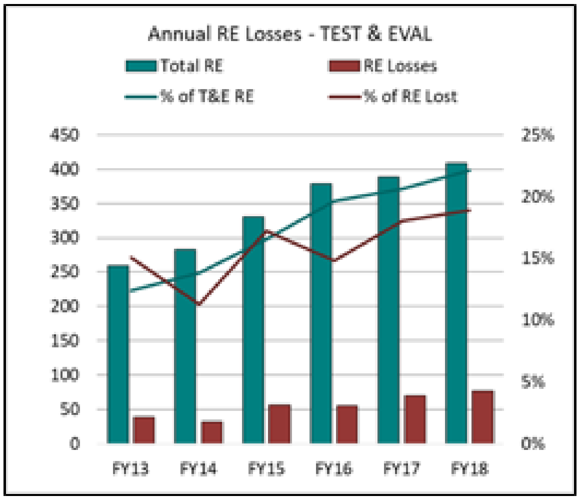


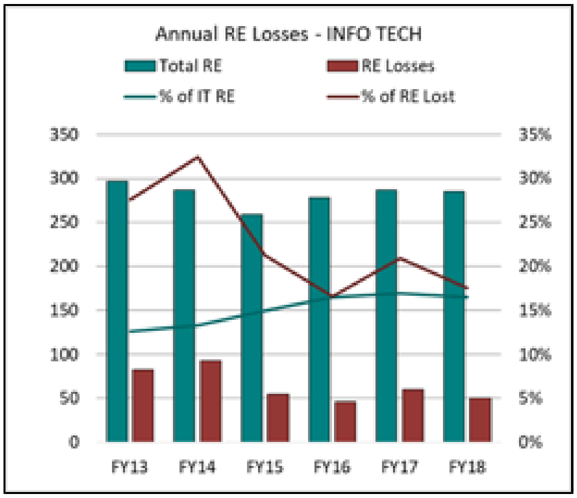


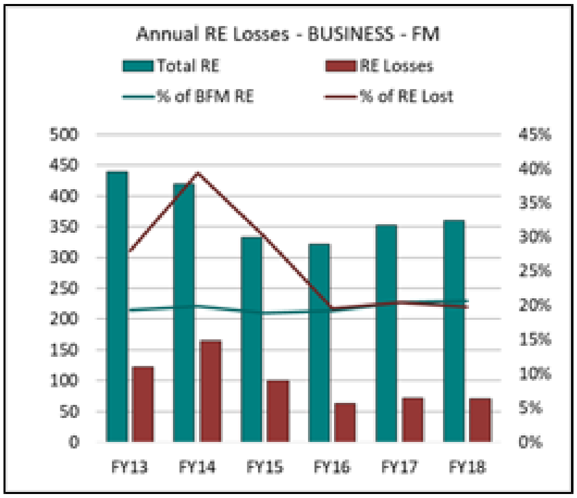


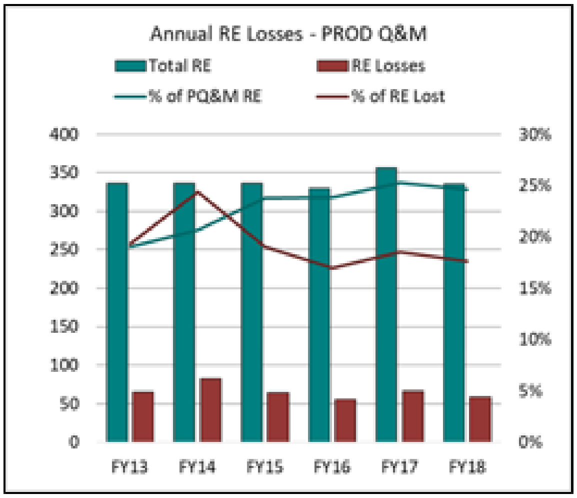


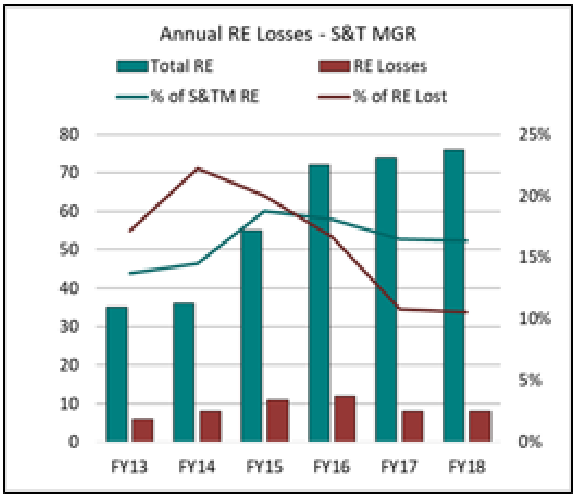


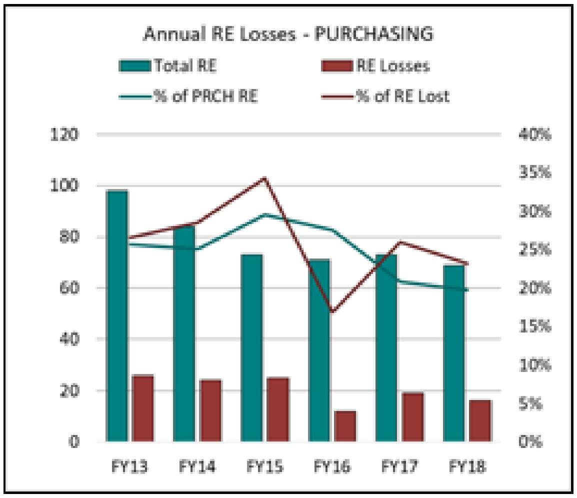


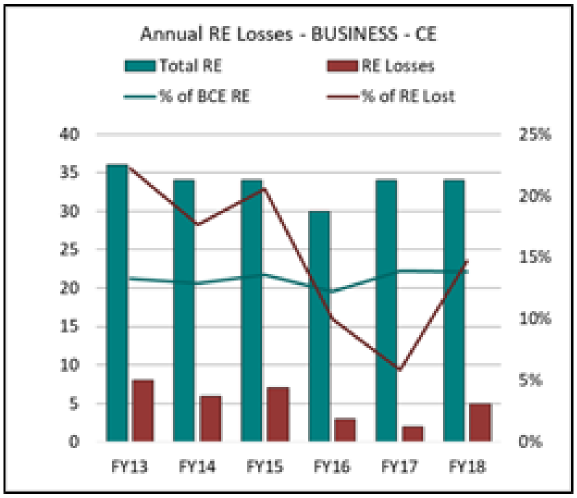

Annual RE Losses - INFO TECH
Total RE
RE Losses
% of IT RE
% of RE Lost
350
300
250
200
150
100
50
0
35%
30%
25%
20%
15%
10%
5%
0%
FY13
FY14
FY15
FY16
FY17
FY18


Annual RE Losses - BUSINESS - FM
Total RE
RE Losses
% of BFM RE
% of RE Lost
500
450
400
350
300
250
200
150
100
50
0
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
FY13
FY14
FY15
FY16
FY17
FY18


Annual RE Losses - PROD Q&M
Total RE
RE Losses
% of PQ&M RE
% of RE Lost
400
350
300
250
200
150
100
50
0
30%
25%
20%
15%
10%
5%
0%
FY13
FY14
FY15
FY16
FY17
FY18


Annual RE Losses - S&T MGR
Total RE
RE Losses
% of S&TM RE
% of RE Lost
80
70
60
50
40
30
20
10
0
25%
20%
15%
10%
5%
0%
FY13
FY14
FY15
FY16
FY17
FY18


Annual RE Losses - PURCHASING
Total RE
RE Losses
% of PRCH RE
% of RE Lost
120
100
80
60
40
20
0
40%
35%
30%
25%
20%
15%
10%
5%
0%
FY13
FY14
FY15
FY16
FY17
FY18


Annual RE Losses - BUSINESS - CE
Total RE
RE Losses
% of BCE RE
% of RE Lost
40
35
30
25
20
15
10
5
0
25%
20%
15%
10%
5%
0%
FY13
FY14
FY15
FY16
FY17
FY18

Enhancing Professional and Technical Excellence: Analysis of Navy Contract Management Competency Models

Rene G. Rendon—is an Associate Professor and Acquisition Management Area Chair in the Graduate School of Business and Public Policy (GSBPP) at the Naval Postgraduate School. A retired Air Force contracting officer, Dr. Rendon served as a warranted contracting officer for major weapons system programs such as the Peacekeeper ICBM, F-22 Advanced Tactical Fighter, Space-Based Infrared Satellite program, and the Evolved Expendable Launch Vehicle program. He also served as a contracting squadron commander for an Air Force pilot training base. He was presented with the Air Force Outstanding Officer in Contracting Award. He has received the NPS Hamming Teaching Excellence Award and the GSBPP Research Excellence Award. Dr. Rendon's research has been published in the *Journal of Purchasing and Supply Management*, *Journal of Defense Analytics and Logistics*, *Journal of Public Procurement*, and the *Journal of Contract Management*. **[**rgrendon@nps.edu**]**

Abstract

The DoD's contracting function continues to be challenged by deficiencies in pre-award, award, and post-award contract management processes. The DoD Inspector General (DoD IG) has identified acquisition and contract management as one of the top 10 DoD Management Challenges for FY2019. Additionally, the Government Accountability Office (GAO) continues to identify DoD contract management as a "high risk" due to the department's challenge in improving the capability of its contract management workforce, specifically ensuring the "workforce has the requisite skills, tools, and training to perform key tasks." Both the DoD IG and the GAO identify the need for increased competency in the DoD contracting workforce.

The DoD's response to these contracting deficiencies and workforce capability challenges continues to be an emphasis on contract management training and workforce competency development. However, recent legislative initiatives reflect Congress's concerns about the adequacy of the DoD's acquisition workforce training and competency development. The FY2016 National Defense Authorization Act (NDAA) Section 809 required the Secretary of Defense to establish an independent advisory panel on streamlining acquisition regulations.

The 809 Panel reported that if the DoD is to achieve its acquisition workforce goals, it will need to prepare and develop its workforce differently. The FY2018 National Defense Authorization Act (NDAA) directed the Under Secretary of Defense (USD) for Acquisition and Sustainment (A&S) to assess the training of the acquisition workforce, specifically, the gaps in business acumen, knowledge of industry operations, and knowledge of industry motivation within the defense acquisition workforce.

Given this background, one must ask: Does the training provided by the DoD truly reflect what is needed by the DoD contracting workforce? The purpose of this research is to conduct an analysis of the DoD contracting competency framework and compare this framework with those of other federal agencies. Additionally, this research will compare the DoD contracting competency model with competency models established by procurement and contracting professional associations. This research builds upon past studies comparing federal government and industry contract management competency frameworks. Based on the analysis and comparisons of the reviewed competency frameworks, recommendations

will be made to improve the DoD contracting competency framework to help improve the professional and technical excellence of the DoD contracting workforce.

Background

The DoD is the federal government's largest contracting agency and obligates approximately $300 billion in contracts every year (GAO, 2019). The DoD contract management workforce is responsible for managing these millions of contract actions for the procurement of mission-critical supplies and services. Yet given the high dollar contract obligations and the importance of these supplies and services to the nation's defense, the DoD's contracting function continues to be challenged by deficiencies in pre-award, award, and post-award contract management processes (DoD, 2009, 2012, 2013a, 2013b, 2014, 2015, 2017). The DoD Inspector General (DoD IG) has identified acquisition and contract management as one of the top 10 DoD Management Challenges for FY2019 (DoD, 2018). Additionally, the Government Accountability Office (GAO) continues to identify DoD contract management as a "high risk" due to the department's challenge in improving the capability of its contract management workforce, specifically ensuring the "workforce has the requisite skills, tools, and training to perform key tasks" (GAO, 2019, p. 228). Thus, both the DoD IG and the GAO identify the need for increased competency in the DoD contracting workforce. In response to these deficiencies in contract management processes, and challenges in improving contract management workforce capability, the DoD continues to emphasize contract management training and workforce competency development.

Recent legislative initiatives reflect Congress's concerns about the adequacy of DoD's acquisition workforce training and competency. For example, the FY2016 National Defense Authorization Act (NDAA) Section 809 required the Secretary of Defense to establish an independent advisory panel on streamlining acquisition regulations. The goals of the Section 809 Panel include: streamlining and improving the efficiency and effectiveness of the defense acquisition process and maintaining defense technology advantage, establishing and administering appropriate buyer and seller relationships in the procurement system, improving the functioning of the acquisition system, and ensuring the continuing financial and ethical integrity of defense procurement programs. In an interim report to Congress, the Section 809 Panel stated that the DoD acquisition workforce was a pivotal factor in the success of acquisition reform and that it should address the acquisition workforce in its analysis and recommendations. The Section 809 Panel also stated that career development needed to be a focus of the Panel's recommendation. Finally, the Panel stated that if the DoD is to achieve its acquisition workforce goals, it will need to prepare and develop its workforce differently (Scott & Thompson, 2019).

Additionally, the FY2018 National Defense Authorization Act (NDAA) directed the Under Secretary of Defense (USD) for Acquisition and Sustainment (A&S) to assess the training of the acquisition workforce. Specifically, the FY2018 NDAA Section 843(c) requires the USD (A&S) to assess gaps in business acumen, knowledge of industry operations, and knowledge of industry motivation within the defense acquisition workforce. NDAA Section 843(c) also required the USD (A&S) to determine the effectiveness of training and development resources offered by providers outside of the DoD that are available to the defense acquisition workforce (NDAA, 2017).

Given this background, one must ask: Does the training provided by the DoD truly reflect what is needed by the DoD contracting workforce? The purpose of this research is to conduct an analysis of the DoD contracting competency framework and compare this framework with those of other federal agencies. Additionally, this research will also compare the DoD contracting competency model with competency models established by procurement and contracting professional associations such as the National Institute for Government Procurement (NIGP) and the National Contract Management Association (NCMA). This research builds upon past studies comparing federal government and industry contract management competency frameworks (Albano, 2013; Rendon & Winn, 2017). This current research will answer the following questions:

- How consistent are the contract management competencies established across the federal government agencies?
- How do the federal government's contracting competencies compare to the contracting competencies established by procurement and contract management professional associations?

Based on the analysis and comparisons of the reviewed competency frameworks, recommendations will be made to improve the DoD contracting competency framework to help improve professional and technical excellence of the DoD contracting workforce. This paper is organized in six sections. The first section provided the background and research purpose of this paper. The following section provides a theoretical framework for the study of the DoD's contracting workforce competency management. After that is a brief discussion of the various contracting competency models across federal agencies and professional associations. Next is a comparison of the federal government contracting competencies with those of professional associations involved in procurement and contract management. In the following section, a summary of comparison findings is provided. The final section concludes with the implications of the research findings and recommendations for the DoD for improving its contracting workforce competency management.

Theoretical Framework

Auditability theory is concerned with those aspects of governance needed by organizations to ensure successful achievement of mission goals and objectives. As organizations focus on proper governance and due diligence in processes and practices, the results include an increased emphasis on auditability in operations. In this sense, auditability is more about "making things auditable" than it is about conducting an audit or an inspection (Power, 1996, p. 289). In making things auditable, organizations establish and actively manage an institutionally acceptable knowledge management system supporting their governance of processes and practices (Power, 1996, 2007). Although auditability is traditionally concerned with an organization's financial operations, auditability theory can also be applied to an organization's contract management operations (Rendon & Rendon, 2015). As organizations increase the contracting out of required supplies and services, the organization's corporate governance structure and the structure's impact on contract success, especially contracts in support of major acquisition projects, have been emerging research topics in the project management literature. Frame (1999) stressed the importance of competent personnel for ensuring the success of an organization's projects and contracts. Rollins and Lanza (2005) discussed the need for a solid corporate governance structure as well as a renewed emphasis on strong internal controls as a response to the increase in project fraud incidents. Crawford and Helm (2009) also discussed governance in public sector organizations and the role projects play in ensuring accountability, transparency, control, compliance, risk management, consistency in delivery, value for money, and stakeholder engagement. Past research has also identified the importance of process capability and process maturity in an organization's ability to achieve its goals and objectives. Rendon (2015) explored the importance of assessing contract management process maturity in U.S. Navy contracting organizations. Frame (1999) and Kerzner (2001) stressed the importance of capable organizational processes for ensuring the success of an organization's projects. The main components of auditability theory, competent personnel, capable processes, and effective internal controls form the basis for auditability theory (Rendon & Rendon, 2015, p. 712). Thus, organizations need a competent workforce, capable processes, and effective internal controls to ensure mission success. Individual competence will lead to greater success in performing contract management tasks and activities just as organizational process maturity will ensure consistent and improved results for the organization (Frame, 1999; Kerzner, 2013; Wysocki, 2004).

The next section provides a brief discussion of the various contracting competency models across federal agencies and professional associations.

Contracting Competency Models

Our research will focus on the two predominant federal government contracting competency models (DoD and FAI) and the two predominant professional association competency models, the National Contract Management Association (NCMA) and the National Institute for Government Procurement (NIGP).

DoD Contracting Competency Model

The DoD implemented the DoDI 5000.66 competency model framework for the contracting career field by establishing its contracting competency model. This model is used to assess the DoD contract management workforce competencies, determine competency gaps, and identify opportunities for training and development to close those competency gaps (OUSD AT&L, 2014). The DoD contracting competency model (hereafter referred to as the DoD model) consists of 11 units of competence (10 technical units and 1 professional unit). The units of competencies are broken down into 28 technical competencies and 10 professional competencies, which are further broken down into 52 technical elements and 10 professional elements (DoD, 2007). The DoD competency model is shown in Appendix A.

Federal Acquisition Institute Contracting Competency Model

The FAI was established in 1976 under the Office of Federal Procurement Policy Act and has been charged with fostering and promoting the development of the civilian agency federal acquisition workforce. The Federal Acquisition Institute Improvement Act of 2011 strengthened the FAI's role to satisfy 12 statutory responsibilities in three broad areas: professional certification training, human capital planning, and acquisition research.

Specifically for the contracting workforce, the FAI developed the Federal Acquisition Certification in Contracting (FAC-C) program. The FAC-C program is for civilian agency federal contracting professionals performing contracting and procurement activities and functions. The purpose of the FAC-C program is to establish general education, training, and experience requirements for those contracting professionals. The FAC-C program is built on competencies that refer to the knowledge, skills, and abilities contracting professionals must have in order to perform their contracting duties. The FAC-C program was revised to better align it with the DoD's Defense Acquisition Workforce Improvement Act (DAWIA) program. The contracting competencies that are the foundation of the FAC-C certification training are the ones developed by the DoD, thus the FAI and DoD share the identical contracting competency framework (FAI, n.d.).

NCMA Contract Management Competency Model

The NCMA contract management competency model is established in the Contract Management Body of Knowledge (CMBOK). The CMBOK was first published in 2002 and has evolved extensively to its current version, published in 2017. The CMBOK is based on the Contract Management Standard (CMS), which was developed through a “voluntary consensus process which included a survey of contract managers, expert drafting, peer review, and formal public comment validation” (NCMA, 2017, p. 20). The purpose of the CMBOK is to “provide a common understanding of the terminology, practices, polices, and processes used in contract management” by both buyers (e.g., government agencies) and sellers (e.g., government contractors; NCMA, 2017, p. 18). The CMBOK competency framework is structured at a sufficient level to apply to all types of government organizations (e.g., federal, state, municipal), as well as industry organizations from all sectors (government, defense, medical, information technology, etc.). The CMBOK accomplishes this purpose through a competency system which consists of seven primary competencies (Leadership, Management, Guiding Principles, Pre-Award, Award, Post-Award, and Learn) and thirty process competencies. The CMS is embedded in the CMBOK and expands on the Pre-Award, Award, and Post-Award competencies by including job tasks for both buyers and sellers. The CMS competencies were developed in alignment with the Federal Acquisition Regulation (FAR). Thus, the CMBOK complements the FAR and can be used by government contract managers and government agencies for development of individual competence as well as organizational capability (Rendon & Winn, 2017). The NCMA competency model (CMBOK) is reflected in Appendix B and the CMS is reflected in Appendix C. The CMS-FAR Matrix is shown in Appendix D.

NIGP Competency Model

The National Institute for Government Procurement (NIGP) has adopted the competence model established by the Universal Public Procurement Certification Council (UPPCC). The UPPCC is an independent entity formed to govern and administer the universal procurement certification programs, specifically the Certified Public Procurement Officer (CPPO) and Certified Professional Public Buyer (CPPB) certifications (UPPCC, 2019). The CPPO and CPPB programs have been adopted by various public procurement professional associations such as NIGP The Institute for Public Procurement, National Association of State Procurement Officers (NASPO), California Association of Public Procurement Officials (CAPPO), and the Florida Association of Public Procurement Officials (FAPPO). The UPPCC has established a body of knowledge (BOK) that governs the skills and competencies needed for the public procurement profession. The BOK was the result of a job task analysis conducted to ensure that the certification exams maintain alignment with the critical skills and knowledge needed for the public procurement profession. The job task analysis process provides assurance that individuals designated by a UPPCC certification possess an essential common body of public procurement knowledge that is objectively assessed and validated by the profession (UPPCC, 2019).

The current UPPCC Body of Knowledge consists of 87 total knowledge statements common to both CPPO and CPPB certifications. The CPPO and CPPB competencies are similar, but differ in how the knowledge is used in both the performance of tasks and the skill level needed. Therefore, the UPPCC developed a BOK for each certification. Both BOKs consist of the following six domain areas: Procurement Administration, Sourcing, Negotiation Process, Contract Administration, Supply Management, and Strategic Procurement Planning. The domain areas consist of 87 common knowledge statements and associated job tasks/responsibilities. The CPPO BOK contains 68 related job tasks/responsibilities and the CPPB BOK contains 61 related job tasks/responsibilities. Appendix E reflects the UPPCC competence model for the CPPO certification (UPPCC, 2019).

Now that we have discussed the DoD competency model (which is identical to the FAI competency model), the NCMA CMBOK, and the UPPCC body of knowledge, we present a comparative analysis of these competency models to identify any similarities and differences among the models. Because the DoD and FAI use the same competency model, the analysis will specifically focus on the DoD, NCMA, and the UPPCC competency models.

4. Comparative Analysis of Contracting Competency Models

The comparative analysis of the contracting competency models will focus on three major areas: structure of competency model, scope of competencies, and supporting documentation.

Structure of Competency Model

The three competency models differ in terms of how they are structured. In this analysis, structure refers to how the competencies are constructed, aligned, and related to each other.

The DoD/FAI competency model's structure (see Appendix A) reflects a mix of contract life cycle phases (Pre-Award and Award, Develop and/or Negotiate Positions, Contract Administration, and Contract Termination), specific procurement areas (Small Business-Socioeconomic Programs, Contracting in a Contingent and/or Combat Environment), and a collection of general competency areas (Other Competencies, Professional Competency). Each unit of competence (11 total) is broken down into individual competencies (38 total), which are then broken down into elements (62 total). Other than this hierarchical relationship between units, competencies, and elements, there is no logical relationship among the competence units. For example, the DoD/FAI model combines both pre-award and award contract life cycle phases into one competency and divides the post-award life cycle phase into two separate competency units of contract administration and contract terminations. As reflected in Appendix A, the units of competence are not structured in any logical arrangement other than just a listing of units of competence.

The NCMA CMBOK (see Appendix B and C) reflects both an extensive hierarchical structure as well as a process flow structure. Hierarchically, each primary competency is broken down into process competencies, which are then broken down into job tasks and sub-tasks. The Guiding Principles competencies are overarching the contract life cycle phases of pre-award, award, and post award phases. Additionally, each contract life cycle phase has its own competency structure. For example, Pre-Award is broken down into Develop Solicitation, which is then broken down into Acquisition Planning and Request Offers. Acquisition Planning can be broken down to five job tasks (Shape Internal Customer Requirements, Conduct Market Research, Perform Risk Analysis, Formulate Contract Strategy, and Finalize Acquisition Plan. These job tasks can also be broken down into sub-tasks. In addition to the Guiding Principles competency, there are supporting competencies such as Leadership and Management. The Management competencies are broken down into the contract management supporting disciplines, which include business management, financial management, project management, risk management, and supply chain management.

The UPPCC model (see Appendix E) is similar in structure to the DoD/FAI model. The UPPCC model reflects a general grouping of procurement functions and activities (Procurement Administration, Supply Management, Strategic Procurement Planning), with some semblance of contract life cycle phases (Sourcing, Negotiation Process, Contract Administration). Each of the six domains consists of a list of knowledge statements and a list of associated tasks/responsibilities. Other than this hierarchical relationship between domains, knowledge statements, and tasks/responsibilities, there is no logical relationship among the domains. As reflected in Appendix D, the domains are not structured in any logical arrangement other than just a listing of categories with knowledge statements and tasks/responsibilities.

Scope of Competency Models

The three competency frameworks differ in terms of the scope of the frameworks. In this analysis, scope refers to the topical coverage of the competencies in the competency model.

The DoD/FAI competency model's scope is focused predominantly on Federal Acquisition Regulation (FAR) governed contracting tasks and activities. Additionally, the DoD/FAI model consists of FAR-based contracting competencies specific to the buying organization's tasks and activities. Furthermore, the DoD/FAI model includes other competencies such as using e-business and automated tools and activity program coordinator for the government purchase card. Finally, the model does include a Professional Competency unit that includes generic competencies such as problem solving, customer service, oral communication, written communication, and other professional skills.

The NCMA CMBOK model is much broader and expanded than the DoD/FAI or the UPPCC competency models. For example, the NCMA CMBOK has a much more broadened focus than just contract management competencies. The CMBOK includes supporting competencies, such as business management, financial management, project management, risk management, and supply chain management, as well as a leadership competency. Additionally, the CMBOK's Learn competency focuses on both individual learning (individual competencies) as well as organizational learning (organizational capability). Finally, and most importantly, the NCMA CMBOK framework expands the contracting life cycle to include both the buyer and seller's competencies, processes, and job tasks. Each contract life cycle phase includes domains for both the buyer and seller. For example, the Pre-Award phase includes the buyer primary competency of Develop Solicitation, which consists of process competencies of Acquisition Planning and Request Offers. The Pre-Award phase also includes the seller primary competency of Develop Offer, which consists of process competencies of Business Development and Develop Win Strategy. Both buyer and seller process competencies are further broken down to buyer job tasks, seller job tasks, and joint job tasks. Thus, the CMBOK framework includes both buyer and seller domains for each phase of the contract life cycle.

The UPPCC body of knowledge model is similar in scope to the DoD/FAI model in that it is focused primarily on government procurement and contracting, specifically from the buyer perspective. Furthermore, the UPPCC includes a domain on Supply Management, with knowledge pertaining to inventory management, asset management, and supply chain management and related tasks and responsibilities. Finally, the UPPCC includes a Strategic Procurement Planning domain, knowledge pertaining to analytical, research, and forecasting techniques, as well as strategic planning and cost/benefit analysis, and related tasks and responsibilities.

Supporting Documentation

The three competency models differ in terms of the amount and type of supporting documentation. In this analysis, supporting documentation refers to the availability of supplemental information and guidance that supports the contracting competency models.

The DoD/FAI competency model is presented in spreadsheet format that consists of separate columns for Units of Competence, Competencies, and Elements. Supplemental information or other supporting documentation related to the DoD/FAI model and its competencies could not be found on DoD or FAI websites.

The NCMA CMBOK model is much more supported by documentation compared to the DoD/FAI and UPPCC frameworks. The NCMA Contract Management Standard (CMS), which is the foundation of the CMBOK, provides the primary competencies for the guiding principles and the life cycle phases, as well as the process competencies and job tasks for both buyer and seller domains of each contract life cycle phase. In addition, the CMBOK document itself provides supporting documentation for the remaining primary and process competencies of Leadership, Management, and Learn, as well as a section on abbreviations, acronyms, and lexicon.

The UPPCC body of knowledge is presented as a four-page document, which provide an introduction and background to the documents, and then lists the domain, knowledge statements, and associate tasks and responsibilities. Supplemental information or other supporting documentation related to the UPPCC bodies of knowledge model and its domains could not be found on the UPPCC website.

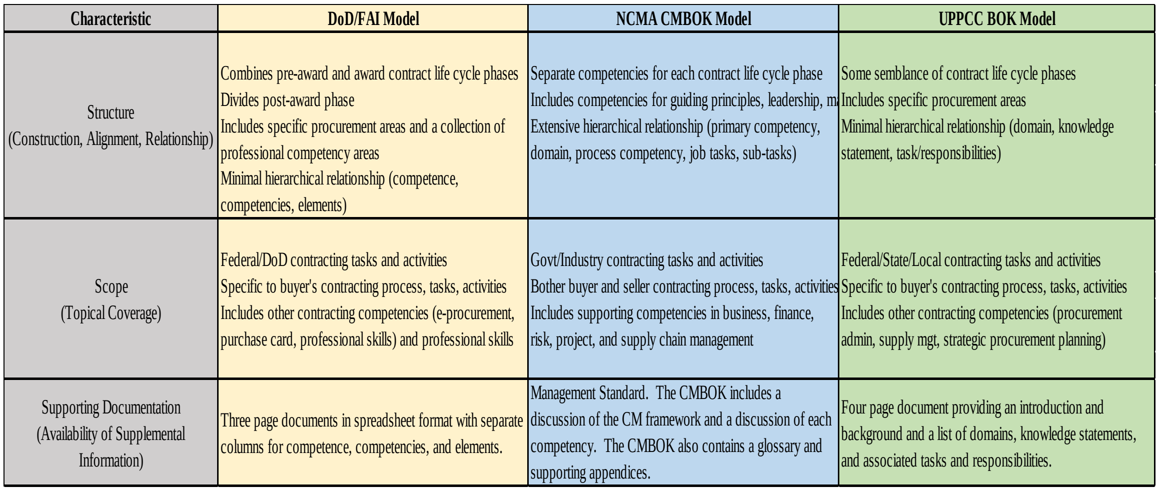
Summary of Comparison Findings

From a summary perspective, the DoD/FAI and UPPCC competency models are similar in terms of structure, scope, and supporting documentation. Both models focus only on government procurement and contract management at the exclusion of any supporting related disciplines. Additionally, both models consist only of contracting competencies from the buyer's perspective. Furthermore, the arrangement of competencies do not include the complete contract life cycle phases in sequence and with sufficient visibility and granularity for each life cycle phase. The DoD/FAI model combines both pre-award and award contract life cycle phases into one competency and divides the post-award life cycle phase into two separate competency units of contract administration and contract terminations. The UPPCC model reflects a general grouping of procurement functions and activities with some semblance of contract life cycle phases. Finally, both the DoD/FAI and UPPCC competency frameworks have minimal supporting documentation.

The NCMA CMBOK competency model is different from the other models in some significant ways. In terms of structure, the CMBOK uses more of a concise life cycle approach with separate competencies for each major contracting life cycle phase, thus providing much more granularity and visibility on pre-award, award, and post-award job tasks and activities. Furthermore, while all reviewed models break down the competencies into lower-level competencies, the CMBOK provides greater granularity and visibility by breaking down each of these life cycle phases into more detailed domains such as acquisition planning and requesting offers (pre-award), conduct negotiations and source selection (award) and administer contracts and contract close out (post-award). Additionally, we conclude that the most significant difference between the reviewed models is that the CMBOK includes competencies related to both buyer and seller perspectives of contract management. Since contract management is about the pre-award, award, and post-award activities performed by both the buyer and seller, it is only appropriate that the CMBOK address the competencies, domains, and job tasks performed by both the buyer and seller. Furthermore, the CMBOK is more broadly structured and includes competencies for supporting disciplines such as business management, project management, financial management, risk management, and supply chain management.

Finally, the CMBOK also includes a Learn competency that focuses on continuous learning at the individual level (competence) and at the organizational level (capability). Our top-level review of the other models does not identify competencies related to organizational capability process capability.

Figure 1 summarizes the results of the comparative analysis showing the major differences between the DoD/FAI, NCMA, and the UPPCC models. These differences may have important implications on contract management workforce professional development, which is discussed in the next section.



Characteristic	DoD/FAI Model	NCMA CMBOK Model	UPPCC BOK Model
Structure (Construction, Alignment, Relationship)	Combines pre-award and award contract life cycle phases Divides post-award phase Includes specific procurement areas and a collection of professional competency areas Minimal hierarchical relationship (competence, competencies, elements)	Separate competencies for each contract life cycle phase Includes competencies for guiding principles, leadership, m Extensive hierarchical relationship (primary competency, domain, process competency, job tasks, sub-tasks)	Some semblance of contract life cycle phases Includes specific procurement areas Minimal hierarchical relationship (domain, knowledge statement, task/responsibilities)
Scope (Topical Coverage)	Federal/DoD contracting tasks and activities Specific to buyer's contracting process, tasks, activities Includes other contracting competencies (e-procurement, purchase card, professional skills) and professional skills	Govt/Industry contracting tasks and activities Bother buyer and seller contracting process, tasks, activities Includes supporting competencies in business, finance, risk, project, and supply chain management	Federal/State/Local contracting tasks and activities Specific to buyer's contracting process, tasks, activities Includes other contracting competencies (procurement admin, supply mgt, strategic procurement planning)
Supporting Documentation (Availability of Supplemental Information)	Three page documents in spreadsheet format with separate columns for competence, competencies, and elements.	Management Standard. The CMBOK includes a discussion of the CM framework and a discussion of each competency. The CMBOK also contains a glossary and supporting appendices.	Four page document providing an introduction and background and a list of domains, knowledge statements, and associated tasks and responsibilities.

Figure 1. **Summary of Comparison Findings**

Implications and Recommendations

The DoD IG continues to identify deficiencies in DoD contract management with past audit reports identifying material internal control weaknesses in contract management processes and procedures. Additionally, the GAO continues to list DoD Contract Management as a high-risk area due to the department's challenges in increasing its contract management workforce capacity to negotiate, manage, and oversee contracts, and to ensure that the workforce has the requisite skills and tools to perform their contract management tasks. Furthermore, past research on the DoD's contract management organizational process capability has identified that post-award contract management processes (e.g., contract administration and contract closeout) are less capable and less mature than the pre-award and award processes (Rendon, 2015). The results of the comparative analysis showing the major differences between the DoD/FAI, NCMA, and UPPCC competency models may provide some insight on how to address these reported contract management deficiencies.

Compared to reviewed competency models, the NCMA CMBOK competency framework may provide a better approach for developing the DoD contracting workforce. Using a more concise and detailed contract life cycle and providing greater emphasis and granularity in each of the contract management phases and tasks (pre-award, award, and post-award) may help develop and fortify the DoD's contract management policies, processes, and practices. Providing greater emphasis on each of the contract life cycle phases and organizing competencies using a hierarchical structure that aligns each competency with processes, job tasks, and sub-tasks would support the development of a professional contracting career path that aligns contracting technical competencies and key work experiences. The recent National Defense Authorization Act (NDAA) for FY2016, Advisory Panel on Streamlining and Codifying Acquisition Regulations (Section 809 Panel), recommended that the DoD create career paths for the contracting functional area that would include such technical competencies and key work experiences.

Expanding the DoD contracting workforce's knowledge to include industry's side of contract management (e.g., industry operations and processes) as reflected in the NCMA CMBOK will help in developing technical and professional skills that can transfer across government and industry, as well as improve communication and collaboration between government and industry. Including the industry side of contracting would also result in strengthening systems thinking within the contract management workforce. Systems thinking "examines the relationship between essential parts of an organization or a problem, and determines how to manage those relationships to get better outcomes" (Carlson, 2017, n.p.). The DoD contracting competency model may be resulting in linear thinking among the contract management workforce, with contract managers believing that contracting problems have "direct causes and that you can optimize the whole by optimizing each of the parts" (Carlson, 2017, n.p.). Contract managers using systems thinking will know that contract management "problems can have hidden, indirect causes" and it is the "relationships among the parts that matter the most" (Carlson, 2017, n.p.). Adopting the NCMA CMBOK for the DoD may provide the DoD contract management workforce with a stronger foundational understanding of not only the complete contract life cycle (pre-award, award, post-award), but also with an understanding of the different perspectives in contractual relationships (e.g., buyer, seller, subcontractors, suppliers, etc.). Using systems thinking, contract managers will be able to "see the gaps where complications or opportunities can arise" within the acquisition process and understand how their contract management strategy decisions may impact contractors and subcontractors (Carlson, 2017, n.p.). Including the seller competencies for the DoD contract management workforce may also strengthen "communication, collaboration, problem-solving, and adaptability" skills (Carlson, 2017, n.p.). The Section 809 Panel recommended that the DoD revise its contracting professional development programs (e.g., professional certifications) to emphasize skills that are transferable across government and industry and focused on a defined set of qualifications connected to contracting positions.

Additionally, there may be value in broadening the DoD's contracting competency model to include other contract management-related disciplines such as business management, financial management, project management, risk management, and supply chain management, as reflected in the NCMA CMBOK. The inclusion of other contract management-related disciplines may enhance the DoD's contracting workforce critical thinking, problem-solving, and analytical skills, bringing increased efficiency to its contract management processes. The Section 809 Panel recommended that the DoD revise its contracting professional development programs (e.g., professional certifications) to emphasize sufficient domain knowledge, emphasize professional skills, and provide a broad perspective to interact effectively with industry. A greater understanding of contract management–related disciplines as well as understanding both government and industry sides of the contract management relationship will help develop "T-shaped" acquisition professionals who have both "depth of knowledge in a particular expertise as well as have the ability to work and communicate across disciplines" (Carlson, 2017, n.p.). T-shaped acquisition professionals will be capable of introducing innovation and process change into the DoD's contract management processes. If the DoD would adopt the NCMA CMBOK, it would achieve a desired recommendation from the 809 Panel that both the DoD and industry would adopt a common body of knowledge, which would also enhance communication and collaboration between government and industry.

Finally, if the DoD emphasized a continuous learning competency at both the individual competence level and also at the organizational capability level, as reflected in the NCMA CMBOK, the DoD may increase its contract management process capability and strengthen its internal controls in contract management processes and procedures. Thus, increasing individual competence, process capability, and internal controls will help in improving auditability in DoD acquisition.

Conclusion

The DoD IG and the GAO continue to identify the need for increased competency in the DoD contracting workforce. The recent Section 809 Panel emphasized the importance of contracting workforce professional development and stated that if the DoD is to achieve its acquisition workforce goals, it will need to prepare and develop its workforce differently. The recent FY2018 NDAA emphasized the need for business acumen, knowledge of industry operations, and knowledge of industry motivation within the defense acquisition workforce. The CMBOK was developed to integrate and standardize common contract management job tasks across the government and industry (NCMA, 2017). When both buyers and sellers understand and interpret contract management terminology, practices, policies, and processes consistently, contract management workforce competence and organizational capability increases, and successful contract management is more likely to be achieved (NCMA, 2017; Rendon & Winn, 2017). Perhaps the DoD should leverage the CMBOK competency model as it continues to emphasize contract management training and continues to develop workforce competencies.

References

Albano, J. D. (2013). *The contract management body of knowledge: A comparison of contracting competencies.* Monterey, CA: Naval Postgraduate School.

Carlson, S. (2017, September 29). A new liberal art: How systems thinking prepares students for a complex world. *Chronicle of Higher Education.*

Crawford, L. H., & Helm, J. (2009). Government and governance: The value of project management in the public sector. *Project Management Journal, 40*(1), 73–87.

DoDIG. (2009). *Summary of DoD Office of Inspector General audits of acquisition and contract administration* (DoDIG Report No. D-2009-071). Washington, DC: DoD.

DoDIG. (2012). *Award and administration of multiple award contracts at naval facilities engineering command specialty centers need improvement* (DODIG-2013-007). Washington, DC: DoD.

DoDIG. (2013a). *Better processes needed to appropriately justify and document NAVSUP WSS, Philadelphia Site sole-source awards* (DODIG-2013-034). Retrieved from http://www.dodig.mil/pubs/documents/DODIG-2013-034.pdf

DoDIG. (2013b, March 21). *Air Force needs better processes to appropriately justify and manage cost-reimbursable contracts* (DODIG-2013-059). Washington, DC: DoD.

DoDIG. (2014). *Navy and Marine Corps have weak procurement processes for cost-reimbursement contract issuance and management* (DODIG-2014-092). Washington, DC: DoD.

DoDIG. (2015, May 15). *Improvements needed for awarding service contracts at Naval Special Warfare Command* (DODIG-2015-124). Washington, DC: DoD.

DoDIG. (2017, March 14). *The Army needs to improve processes for single-award, indefinite-delivery indefinite-quantity contracts* (DODIG-2017-065). Washington, DC: DoD.

DoDIG. (2018). *Fiscal Year 2019 top DoD management challenges*. Washington, DC: DoD.

Federal Acquisition Institute. (n.d.). *Contracting competencies.* Retrieved from http://www.fai.gov/drupal/certification/contracting-competencies#tech

Frame, D. L. (1999). *Project management competence: Building key skills for individuals, teams, and organizations.* San Francisco, CA: Jossey-Bass.

GAO. (2019). *High-risk series: Substantial efforts needed to achieve greater progress on high-risk series* (GAO-19-157SP). Washington, DC: Author.

Kerzner, H. (2001). *Strategic planning for project management using a project management maturity model.* New York, NY: John Wiley & Sons.

Kerzner, H. R. (2013). *Project management: A systems approach to planning, scheduling, and controlling.* Hoboken, NJ: Wiley.

Power, M. (1996). Making things auditable. *Accounting, Organizations and Society, 21*(2), 289–315.

Power, M. (2007). *Organizations and auditability: A theory* (Vol. 9). Lancaster, England: Lancaster University.

National Contract Management Association (NCMA). (2016). *Contract management standard (CMS)*. Ashburn, VA: Author. Retrieved from http://www.ncmahq.org/docs/default-source/default-document-library/pdfs/the-contract-management-standard.pdf?sfvrsn=37b90f2b_10

National Contract Management Association (NCMA). (2017). *Contract management body of knowledge (CMBOK)* (5th ed.). Ashburn, VA: Author.

National Defense Authorization Act (NDAA) for Fiscal Year 2018, Pub. L. No. 115-91 (December 12, 2017). Retrieved from https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf

Office of the Under Secretary of Defense (AT&L). (2014). *Competency assessment of the contracting career field*. Washington, DC: Defense Procurement and Acquisition Policy Office. Retrieved from https://www.acq.osd.mil/dpap/ops/contracting_competency_assessment.html

Rendon, R. G. (2015). Benchmarking contract management process maturity: A case study of the US Navy. *Benchmarking: An International Journal, 22*(7), 1481–1508.

Rendon, R. G., & Rendon, J. M. (2015). Auditability in public procurement: An analysis of internal controls and fraud vulnerability. *International Journal of Procurement Management, 8*(6), 710–730.

Rendon, R. G., & Winn, T. (2017, December). Competency in contract management: A comparison of DOD and CMBOK competency models. *Contract Management, 57*(12), 66–81.

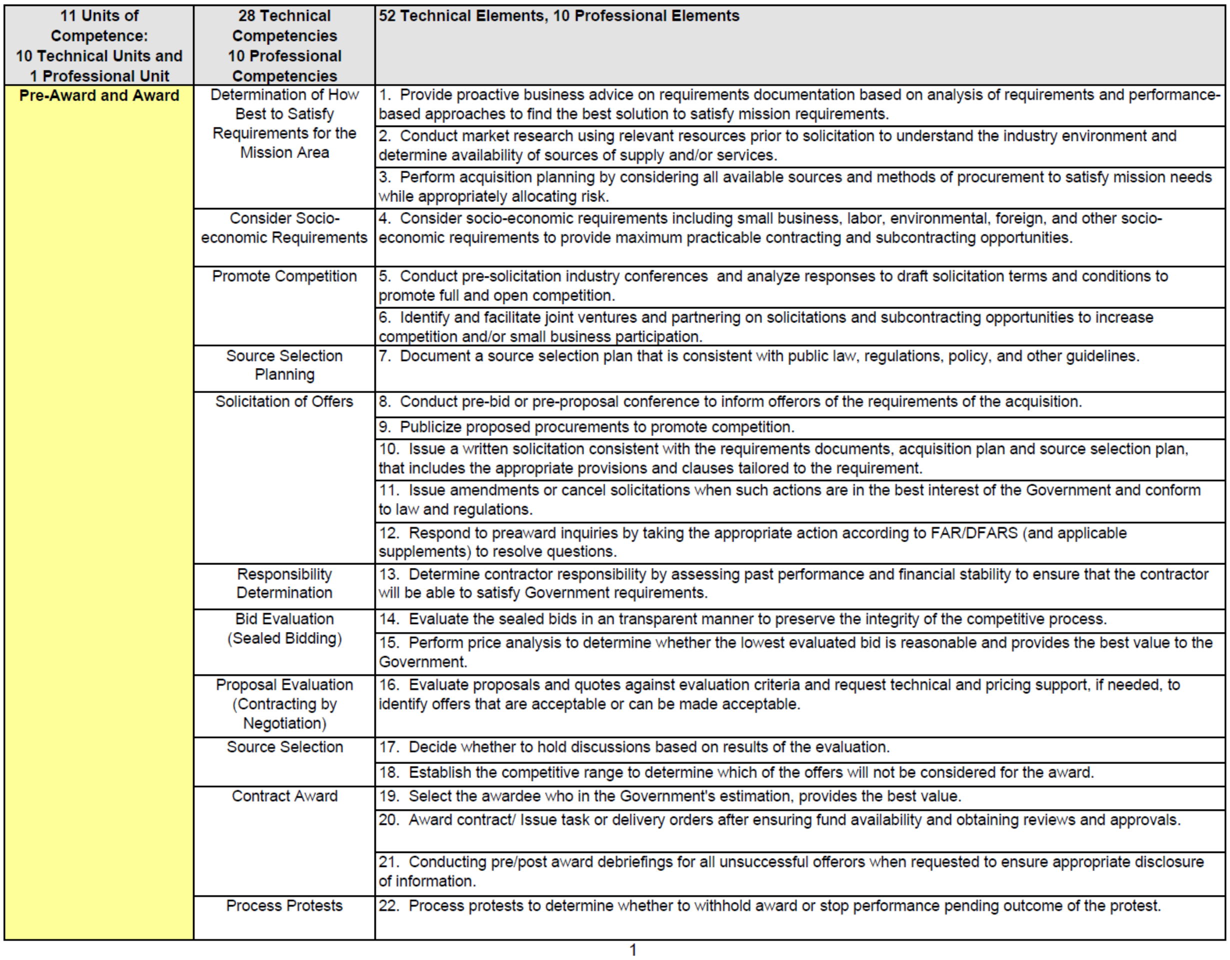
Rollins, S. C., & Lanza, R. B. (2005). *Essential project investment governance and reporting: Preventing project fraud and ensuring Sarbanes-Oxley Compliance*. Ft. Lauderdale, FL: J. Ross Publishing.

Scott, D., & Thompson, D. (2019, January). Toward building the DoD acquisition workforce of the twenty-first century: Recommendations of the Section 809 Panel on Professional Development. *Contract Management*.

Universal Public Procurement Certification Council (UPPCC). (2019). UPPCC Body of Knowledge. Retrieved from https://www.uppcc.org/certified/2013-body-knowledge

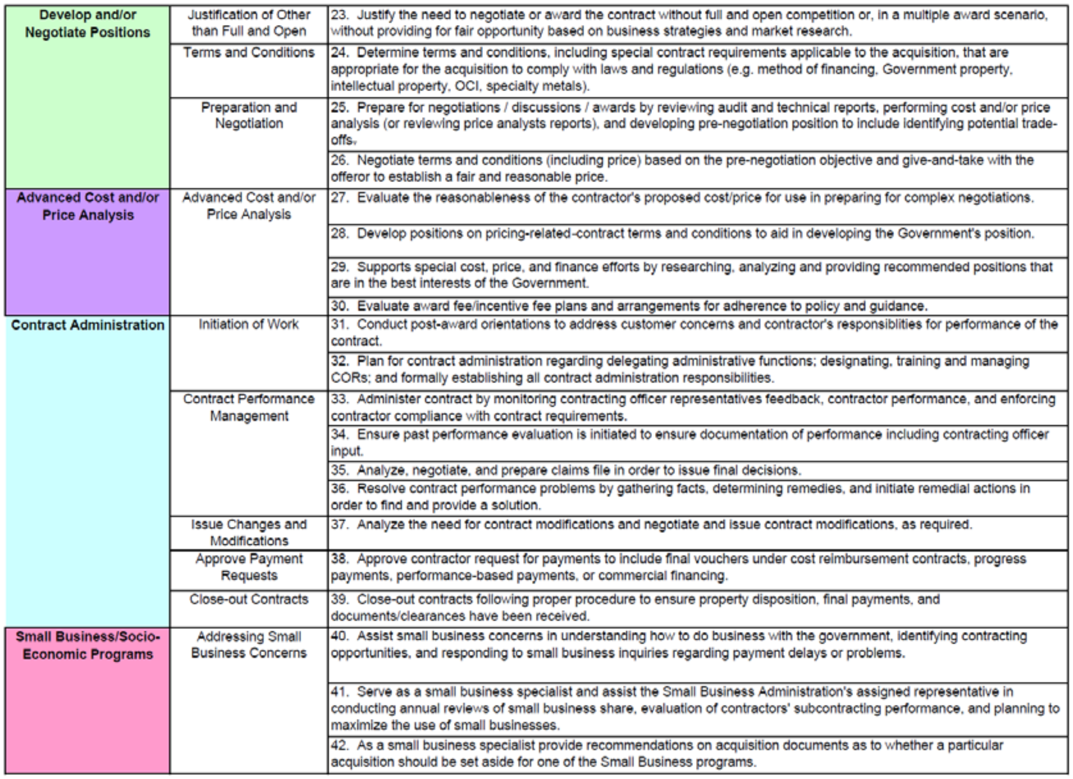
Wysocki, R. K. (2004). *Project management process improvement*. Norwood, MA: Artech House.

Appendix A. DoD Contracting Competency Model



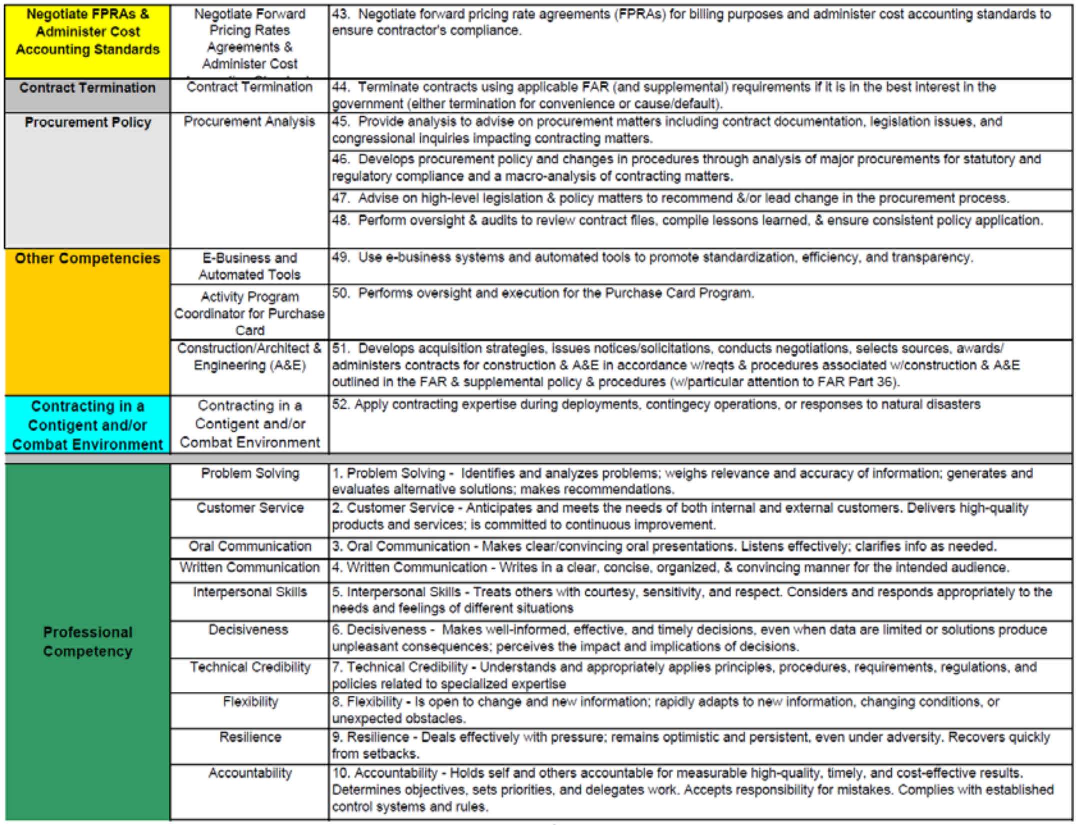
11 Units of Competence: 10 Technical Units and 1 Professional Unit	28 Technical Competencies 10 Professional Competencies	52 Technical Elements, 10 Professional Elements
Pre-Award and Award	Determination of How Best to Satisfy Requirements for the Mission Area	1. Provide proactive business advice on requirements documentation based on analysis of requirements and performance-based approaches to find the best solution to satisfy mission requirements.
		2. Conduct market research using relevant resources prior to solicitation to understand the industry environment and determine availability of sources of supply and/or services.
		3. Perform acquisition planning by considering all available sources and methods of procurement to satisfy mission needs while appropriately allocating risk.
	Consider Socio-economic Requirements	4. Consider socio-economic requirements including small business, labor, environmental, foreign, and other socio-economic requirements to provide maximum practicable contracting and subcontracting opportunities.
	Promote Competition	5. Conduct pre-solicitation industry conferences and analyze responses to draft solicitation terms and conditions to promote full and open competition.
		6. Identify and facilitate joint ventures and partnering on solicitations and subcontracting opportunities to increase competition and/or small business participation.
	Source Selection Planning	7. Document a source selection plan that is consistent with public law, regulations, policy, and other guidelines.
	Solicitation of Offers	8. Conduct pre-bid or pre-proposal conference to inform offerors of the requirements of the acquisition.
		9. Publicize proposed procurements to promote competition.
		10. Issue a written solicitation consistent with the requirements documents, acquisition plan and source selection plan, that includes the appropriate provisions and clauses tailored to the requirement.
		11. Issue amendments or cancel solicitations when such actions are in the best interest of the Government and conform to law and regulations.
		12. Respond to preaward inquiries by taking the appropriate action according to FAR/DFARS (and applicable supplements) to resolve questions.
	Responsibility Determination	13. Determine contractor responsibility by assessing past performance and financial stability to ensure that the contractor will be able to satisfy Government requirements.
	Bid Evaluation (Sealed Bidding)	14. Evaluate the sealed bids in an transparent manner to preserve the integrity of the competitive process.
		15. Perform price analysis to determine whether the lowest evaluated bid is reasonable and provides the best value to the Government.
	Proposal Evaluation (Contracting by Negotiation)	16. Evaluate proposals and quotes against evaluation criteria and request technical and pricing support, if needed, to identify offers that are acceptable or can be made acceptable.
	Source Selection	17. Decide whether to hold discussions based on results of the evaluation.
		18. Establish the competitive range to determine which of the offers will not be considered for the award.
	Contract Award	19. Select the awardee who in the Government's estimation, provides the best value.
		20. Award contract/ Issue task or delivery orders after ensuring fund availability and obtaining reviews and approvals.
		21. Conducting pre/post award debriefings for all unsuccessful offerors when requested to ensure appropriate disclosure of information.
	Process Protests	22. Process protests to determine whether to withhold award or stop performance pending outcome of the protest.

1



Develop and/or Negotiate Positions	Justification of Other than Full and Open	23. Justify the need to negotiate or award the contract without full and open competition or, in a multiple award scenario, without providing for fair opportunity based on business strategies and market research.
	Terms and Conditions	24. Determine terms and conditions, including special contract requirements applicable to the acquisition, that are appropriate for the acquisition to comply with laws and regulations (e.g. method of financing, Government property, intellectual property, OCI, specialty metals).
	Preparation and Negotiation	25. Prepare for negotiations / discussions / awards by reviewing audit and technical reports, performing cost and/or price analysis (or reviewing price analysts reports), and developing pre-negotiation position to include identifying potential trade-offs.
		26. Negotiate terms and conditions (including price) based on the pre-negotiation objective and give-and-take with the offeror to establish a fair and reasonable price.
Advanced Cost and/or Price Analysis	Advanced Cost and/or Price Analysis	27. Evaluate the reasonableness of the contractor's proposed cost/price for use in preparing for complex negotiations.
		28. Develop positions on pricing-related-contract terms and conditions to aid in developing the Government's position.
		29. Supports special cost, price, and finance efforts by researching, analyzing and providing recommended positions that are in the best interests of the Government.
		30. Evaluate award fee/incentive fee plans and arrangements for adherence to policy and guidance.
Contract Administration	Initiation of Work	31. Conduct post-award orientations to address customer concerns and contractor's responsiblities for performance of the contract.
		32. Plan for contract administration regarding delegating administrative functions; designating, training and managing CORs; and formally establishing all contract administration responsibilities.
	Contract Performance Management	33. Administer contract by monitoring contracting officer representatives feedback, contractor performance, and enforcing contractor compliance with contract requirements.
		34. Ensure past performance evaluation is initiated to ensure documentation of performance including contracting officer input.
		35. Analyze, negotiate, and prepare claims file in order to issue final decisions.
		36. Resolve contract performance problems by gathering facts, determining remedies, and initiate remedial actions in order to find and provide a solution.
	Issue Changes and Modifications	37. Analyze the need for contract modifications and negotiate and issue contract modifications, as required.
	Approve Payment Requests	38. Approve contractor request for payments to include final vouchers under cost reimbursement contracts, progress payments, performance-based payments, or commercial financing.
	Close-out Contracts	39. Close-out contracts following proper procedure to ensure property disposition, final payments, and documents/clearances have been received.
Small Business/Socio-Economic Programs	Addressing Small Business Concerns	40. Assist small business concerns in understanding how to do business with the government, identifying contracting opportunities, and responding to small business inquiries regarding payment delays or problems.
		41. Serve as a small business specialist and assist the Small Business Administration's assigned representative in conducting annual reviews of small business share, evaluation of contractors' subcontracting performance, and planning to maximize the use of small businesses.
		42. As a small business specialist provide recommendations on acquisition documents as to whether a particular acquisition should be set aside for one of the Small Business programs.

2

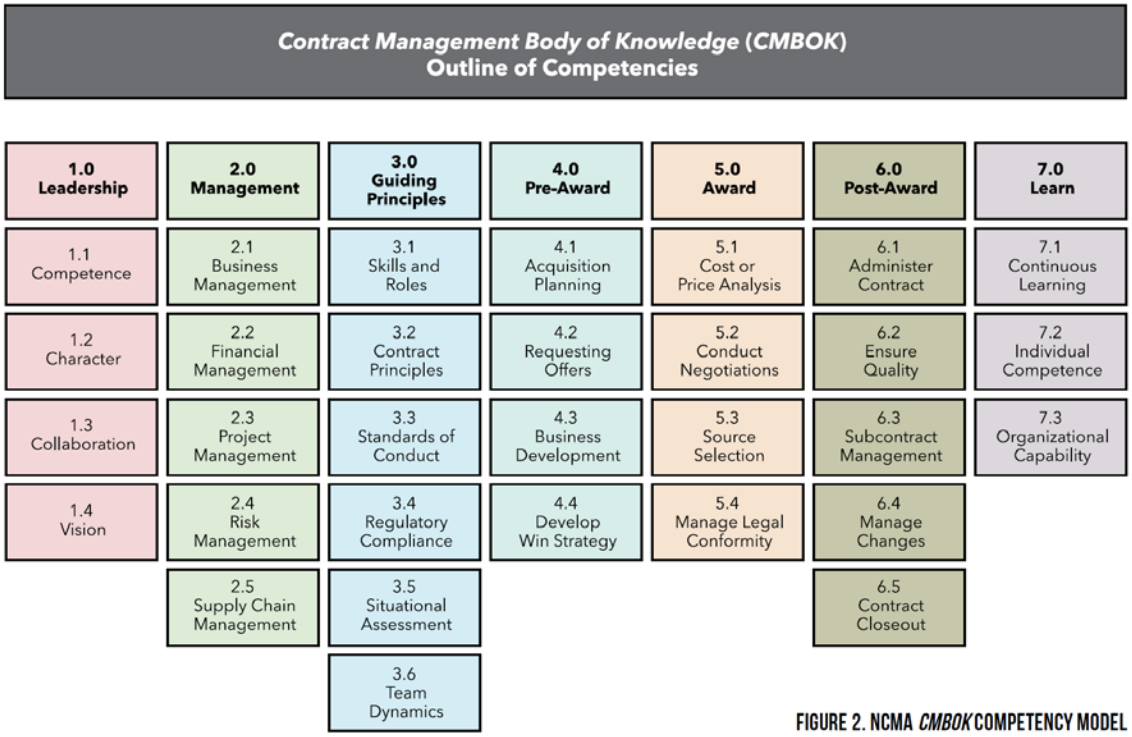


Negotiate FPRAs & Administer Cost Accounting Standards	Negotiate Forward Pricing Rates Agreements & Administer Cost	43. Negotiate forward pricing rate agreements (FPRAs) for billing purposes and administer cost accounting standards to ensure contractor's compliance.
Contract Termination	Contract Termination	44. Terminate contracts using applicable FAR (and supplemental) requirements if it is in the best interest in the government (either termination for convenience or cause/default).
Procurement Policy	Procurement Analysis	45. Provide analysis to advise on procurement matters including contract documentation, legislation issues, and congressional inquiries impacting contracting matters.
		46. Develops procurement policy and changes in procedures through analysis of major procurements for statutory and regulatory compliance and a macro-analysis of contracting matters.
		47. Advise on high-level legislation & policy matters to recommend &/or lead change in the procurement process.
		48. Perform oversight & audits to review contract files, compile lessons learned, & ensure consistent policy application.
Other Competencies	E-Business and Automated Tools	49. Use e-business systems and automated tools to promote standardization, efficiency, and transparency.
	Activity Program Coordinator for Purchase Card	50. Performs oversight and execution for the Purchase Card Program.
	Construction/Architect & Engineering (A&E)	51. Develops acquisition strategies, issues notices/solicitations, conducts negotiations, selects sources, awards/ administers contracts for construction & A&E in accordance w/reqts & procedures associated w/construction & A&E outlined in the FAR & supplemental policy & procedures (w/particular attention to FAR Part 36).
Contracting in a Contigent and/or Combat Environment	Contracting in a Contigent and/or Combat Environment	52. Apply contracting expertise during deployments, contingecy operations, or responses to natural disasters
Professional Competency	Problem Solving	1. Problem Solving - Identifies and analyzes problems; weighs relevance and accuracy of information; generates and evaluates alternative solutions; makes recommendations.
	Customer Service	2. Customer Service - Anticipates and meets the needs of both internal and external customers. Delivers high-quality products and services; is committed to continuous improvement.
	Oral Communication	3. Oral Communication - Makes clear/convincing oral presentations. Listens effectively; clarifies info as needed.
	Written Communication	4. Written Communication - Writes in a clear, concise, organized, & convincing manner for the intended audience.
	Interpersonal Skills	5. Interpersonal Skills - Treats others with courtesy, sensitivity, and respect. Considers and responds appropriately to the needs and feelings of different situations
	Decisiveness	6. Decisiveness - Makes well-informed, effective, and timely decisions, even when data are limited or solutions produce unpleasant consequences; perceives the impact and implications of decisions.
	Technical Credibility	7. Technical Credibility - Understands and appropriately applies principles, procedures, requirements, regulations, and policies related to specialized expertise
	Flexibility	8. Flexibility - Is open to change and new information; rapidly adapts to new information, changing conditions, or unexpected obstacles.
	Resilience	9. Resilience - Deals effectively with pressure; remains optimistic and persistent, even under adversity. Recovers quickly from setbacks.
	Accountability	10. Accountability - Holds self and others accountable for measurable high-quality, timely, and cost-effective results. Determines objectives, sets priorities, and delegates work. Accepts responsibility for mistakes. Complies with established control systems and rules.

3

Appendix B. NCMA CMBOK Competency Model

(NCMA, 2017)



Contract Management Body of Knowledge (CMBOK)
Outline of Competencies

1.0 Leadership	**2.0 Management**	**3.0 Guiding Principles**	**4.0 Pre-Award**	**5.0 Award**	**6.0 Post-Award**	**7.0 Learn**
1.1 Competence	2.1 Business Management	3.1 Skills and Roles	4.1 Acquisition Planning	5.1 Cost or Price Analysis	6.1 Administer Contract	7.1 Continuous Learning
1.2 Character	2.2 Financial Management	3.2 Contract Principles	4.2 Requesting Offers	5.2 Conduct Negotiations	6.2 Ensure Quality	7.2 Individual Competence
1.3 Collaboration	2.3 Project Management	3.3 Standards of Conduct	4.3 Business Development	5.3 Source Selection	6.3 Subcontract Management	7.3 Organizational Capability
1.4 Vision	2.4 Risk Management	3.4 Regulatory Compliance	4.4 Develop Win Strategy	5.4 Manage Legal Conformity	6.4 Manage Changes	
	2.5 Supply Chain Management	3.5 Situational Assessment			6.5 Contract Closeout	
		3.6 Team Dynamics				

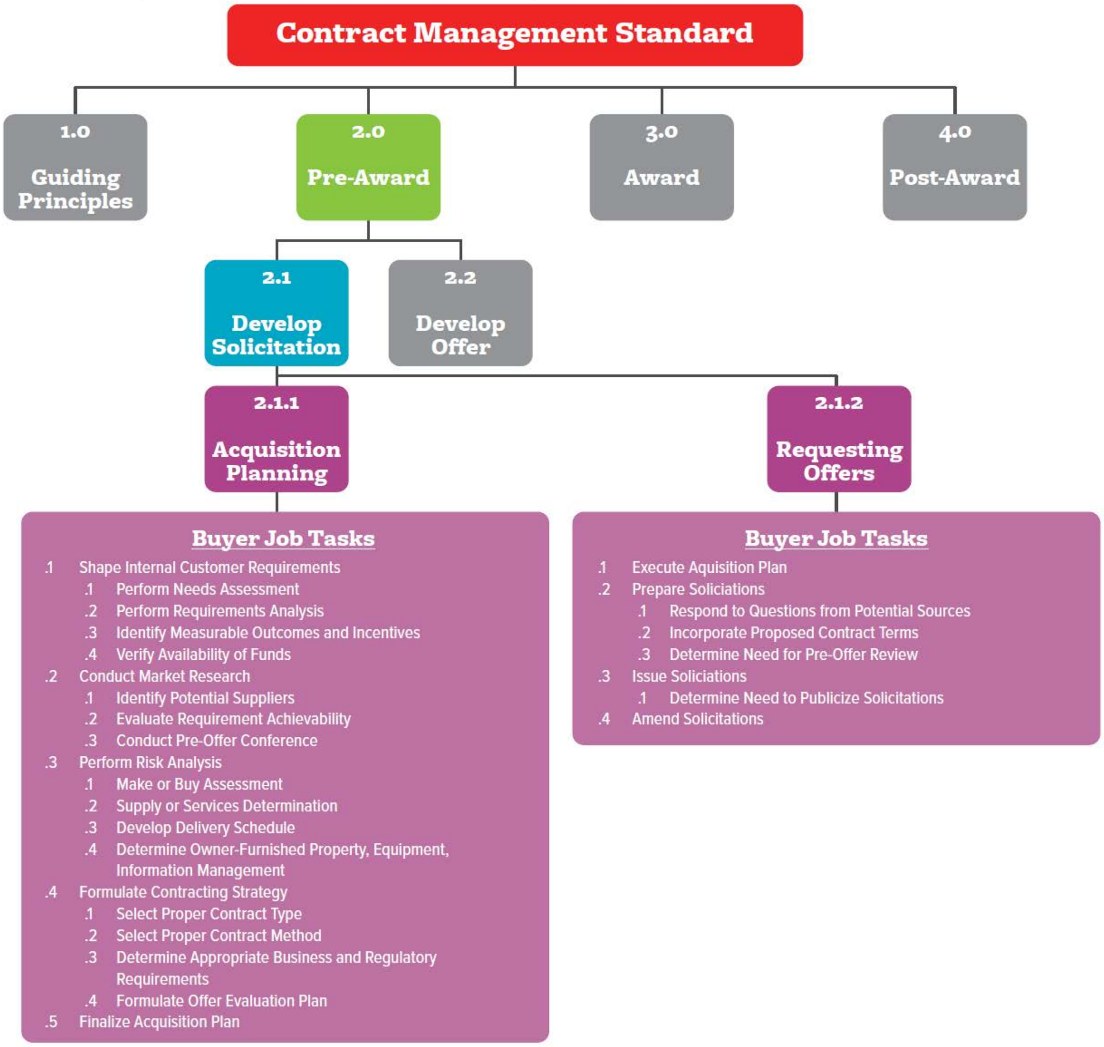
FIGURE 2. NCMA *CMBOK* COMPETENCY MODEL

Note. Used by permission.

Appendix C. NCMA Contract Management Standard (CMS)

(NCMA, 2016)

FIGURE 8. Competencies and Tasks for the *Develop Solicitation* Domain



Buyer Job Tasks

.1 Shape Internal Customer Requirements
- .1 Perform Needs Assessment
- .2 Perform Requirements Analysis
- .3 Identify Measurable Outcomes and Incentives
- .4 Verify Availability of Funds

.2 Conduct Market Research
- .1 Identify Potential Suppliers
- .2 Evaluate Requirement Achievability
- .3 Conduct Pre-Offer Conference

.3 Perform Risk Analysis
- .1 Make or Buy Assessment
- .2 Supply or Services Determination
- .3 Develop Delivery Schedule
- .4 Determine Owner-Furnished Property, Equipment, Information Management

.4 Formulate Contracting Strategy
- .1 Select Proper Contract Type
- .2 Select Proper Contract Method
- .3 Determine Appropriate Business and Regulatory Requirements
- .4 Formulate Offer Evaluation Plan

.5 Finalize Acquisition Plan

Buyer Job Tasks

.1 Execute Aquisition Plan

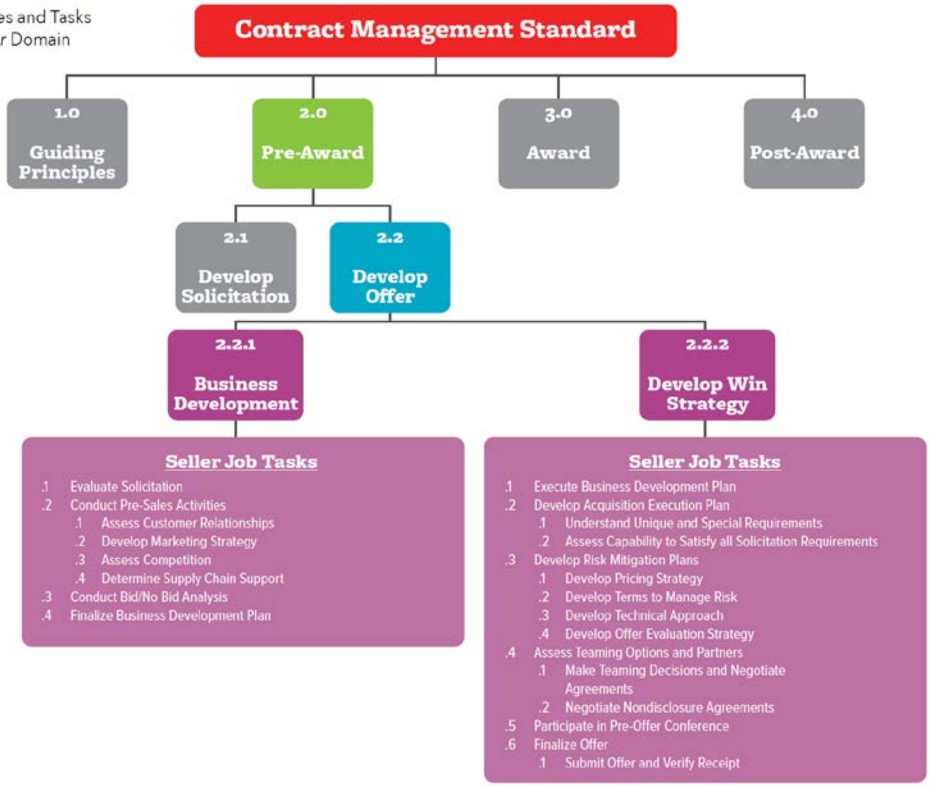
.2 Prepare Soliciations
- .1 Respond to Questions from Potential Sources
- .2 Incorporate Proposed Contract Terms
- .3 Determine Need for Pre-Offer Review

.3 Issue Soliciations
- .1 Determine Need to Publicize Solicitations

.4 Amend Solicitations

Note. Used by permission.

FIGURE 9. Competencies and Tasks for the *Develop Offer* Domain



Seller Job Tasks (2.2.1 Business Development)

.1 Evaluate Solicitation
.2 Conduct Pre-Sales Activities
  .1 Assess Customer Relationships
  .2 Develop Marketing Strategy
  .3 Assess Competition
  .4 Determine Supply Chain Support
.3 Conduct Bid/No Bid Analysis
.4 Finalize Business Development Plan

Seller Job Tasks (2.2.2 Develop Win Strategy)

.1 Execute Business Development Plan
.2 Develop Acquisition Execution Plan
  .1 Understand Unique and Special Requirements
  .2 Assess Capability to Satisfy all Solicitation Requirements
.3 Develop Risk Mitigation Plans
  .1 Develop Pricing Strategy
  .2 Develop Terms to Manage Risk
  .3 Develop Technical Approach
  .4 Develop Offer Evaluation Strategy
.4 Assess Teaming Options and Partners
  .1 Make Teaming Decisions and Negotiate Agreements
  .2 Negotiate Nondisclosure Agreements
.5 Participate in Pre-Offer Conference
.6 Finalize Offer
  .1 Submit Offer and Verify Receipt

FIGURE 10. Competencies and Tasks for the *Form Contract* Domain

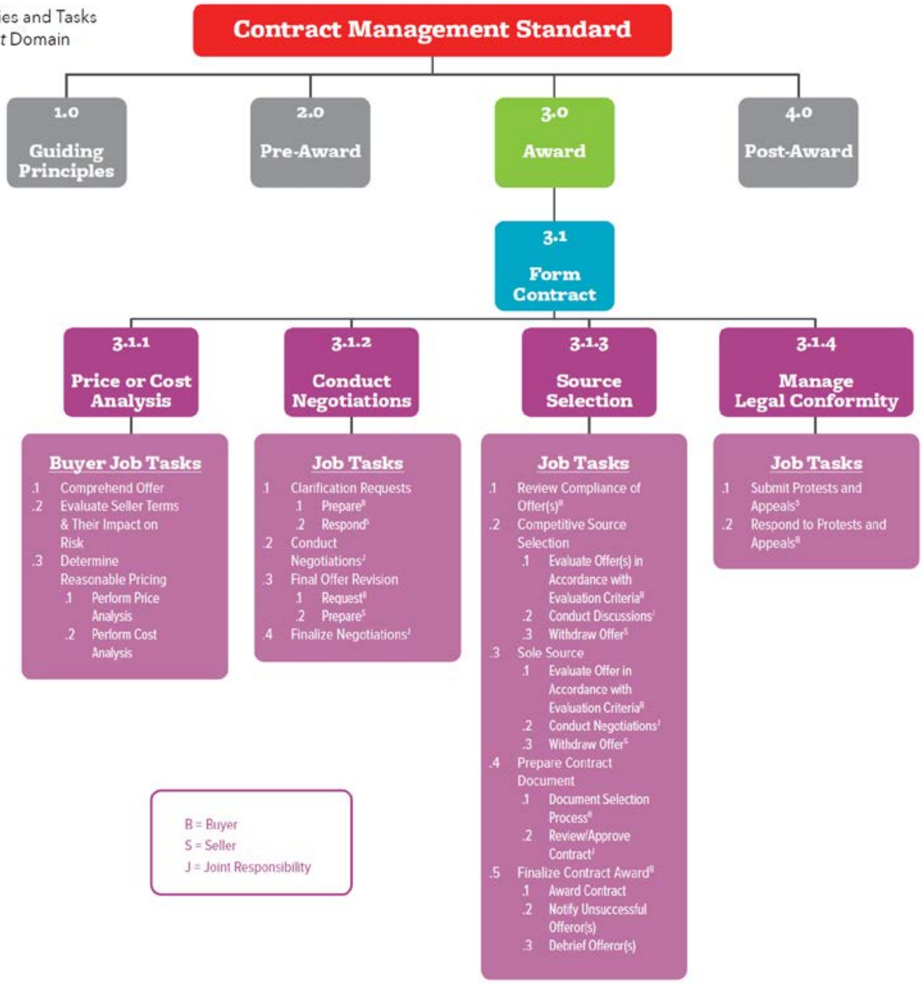
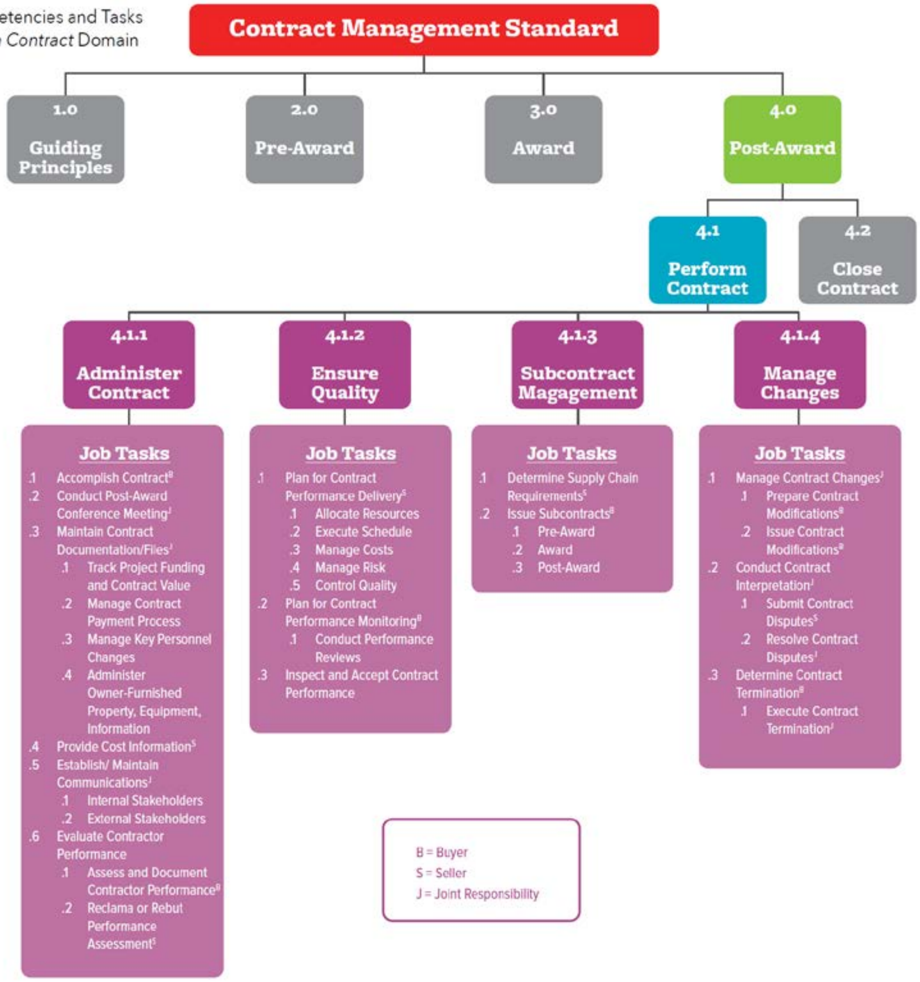

Contract Management Standard
1.0 Guiding Principles
2.0 Pre-Award
3.0 Award
4.0 Post-Award
3.1 Form Contract
3.1.1 Price or Cost Analysis
3.1.2 Conduct Negotiations
3.1.3 Source Selection
3.1.4 Manage Legal Conformity
Buyer Job Tasks
.1 Comprehend Offer
.2 Evaluate Seller Terms & Their Impact on Risk
.3 Determine Reasonable Pricing
.1 Perform Price Analysis
.2 Perform Cost Analysis
Job Tasks
.1 Clarification Requests
.1 Prepare^{B}
.2 Respond^{S}
.2 Conduct Negotiations^{J}
.3 Final Offer Revision
.1 Request^{B}
.2 Prepare^{S}
.4 Finalize Negotiations^{J}
Job Tasks
.1 Review Compliance of Offer(s)^{B}
.2 Competitive Source Selection
.1 Evaluate Offer(s) in Accordance with Evaluation Criteria^{B}
.2 Conduct Discussions^{J}
.3 Withdraw Offer^{S}
.3 Sole Source
.1 Evaluate Offer in Accordance with Evaluation Criteria^{B}
.2 Conduct Negotiations^{J}
.3 Withdraw Offer^{S}
.4 Prepare Contract Document
.1 Document Selection Process^{B}
.2 Review/Approve Contract^{J}
.5 Finalize Contract Award^{B}
.1 Award Contract
.2 Notify Unsuccessful Offeror(s)
.3 Debrief Offeror(s)
Job Tasks
.1 Submit Protests and Appeals^{S}
.2 Respond to Protests and Appeals^{B}
B = Buyer
S = Seller
J = Joint Responsibility

FIGURE 11. Competencies and Tasks for the *Perform Contract* Domain


Contract Management Standard
1.0
Guiding Principles
2.0
Pre-Award
3.0
Award
4.0
Post-Award
4.1
Perform Contract
4.2
Close Contract
4.1.1
Administer Contract
4.1.2
Ensure Quality
4.1.3
Subcontract Magagement
4.1.4
Manage Changes
Job Tasks
.1 Accomplish Contract^{B}
.2 Conduct Post-Award Conference Meeting^{J}
.3 Maintain Contract Documentation/Files^{J}
.1 Track Project Funding and Contract Value
.2 Manage Contract Payment Process
.3 Manage Key Personnel Changes
.4 Administer Owner-Furnished Property, Equipment, Information
.4 Provide Cost Information^{S}
.5 Establish/ Maintain Communications^{J}
.1 Internal Stakeholders
.2 External Stakeholders
.6 Evaluate Contractor Performance
.1 Assess and Document Contractor Performance^{B}
.2 Reclama or Rebut Performance Assessment^{S}
Job Tasks
.1 Plan for Contract Performance Delivery^{S}
.1 Allocate Resources
.2 Execute Schedule
.3 Manage Costs
.4 Manage Risk
.5 Control Quality
.2 Plan for Contract Performance Monitoring^{B}
.1 Conduct Performance Reviews
.3 Inspect and Accept Contract Performance
Job Tasks
.1 Determine Supply Chain Requirements^{S}
.2 Issue Subcontracts^{B}
.1 Pre-Award
.2 Award
.3 Post-Award
Job Tasks
.1 Manage Contract Changes^{J}
.1 Prepare Contract Modifications^{B}
.2 Issue Contract Modifications^{B}
.2 Conduct Contract Interpretation^{J}
.1 Submit Contract Disputes^{S}
.2 Resolve Contract Disputes^{J}
.3 Determine Contract Termination^{B}
.1 Execute Contract Termination^{J}
B = Buyer
S = Seller
J = Joint Responsibility

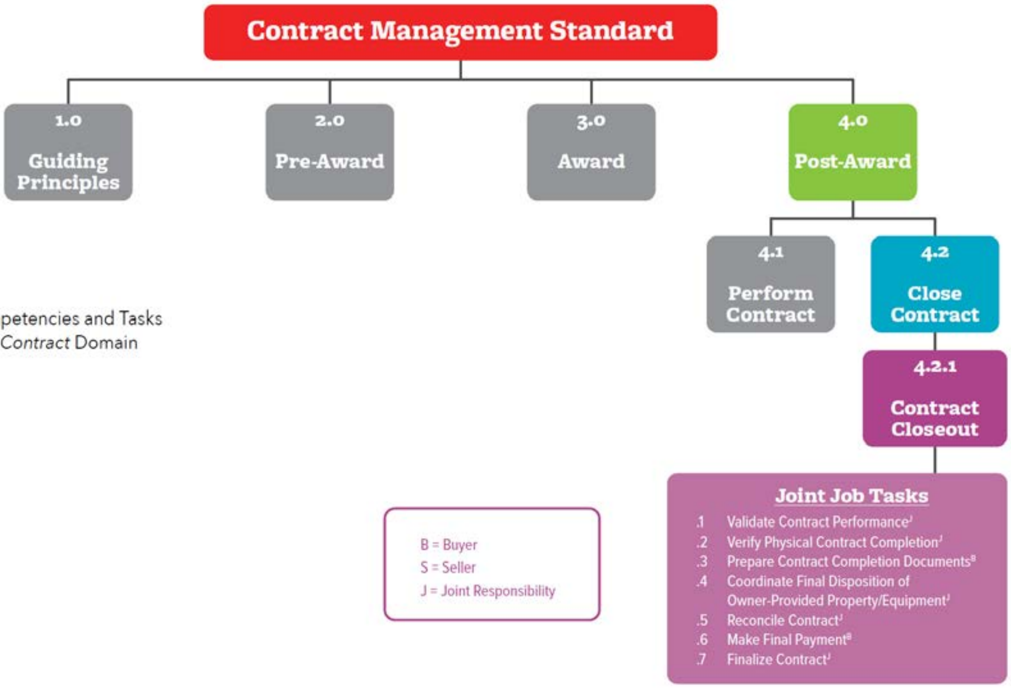
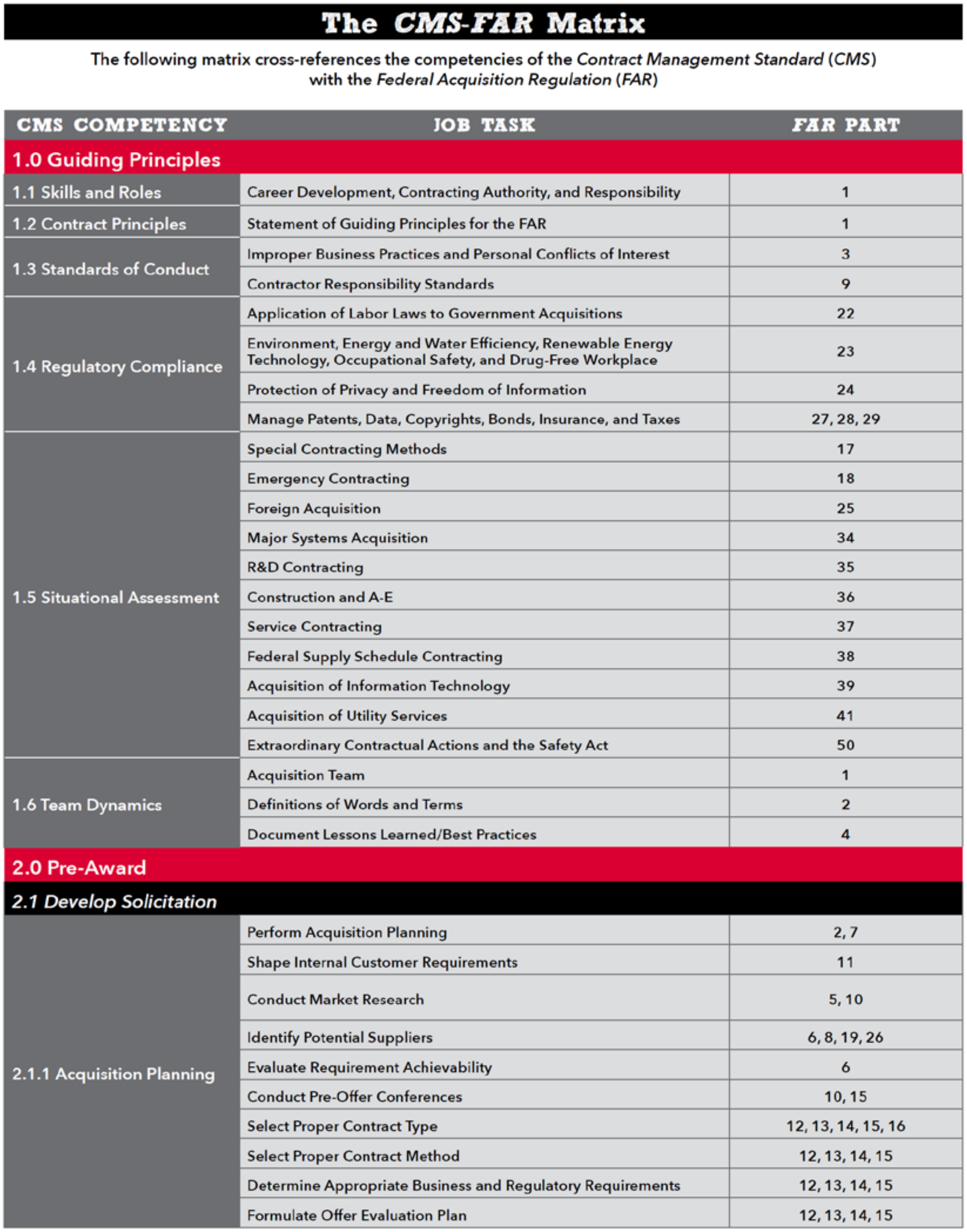


FIGURE 12. Competencies and Tasks for the *Close Contract* Domain

Appendix D. NCMA Contract Management Standard—FAR Matrix

(Rendon & Winn, 2017)

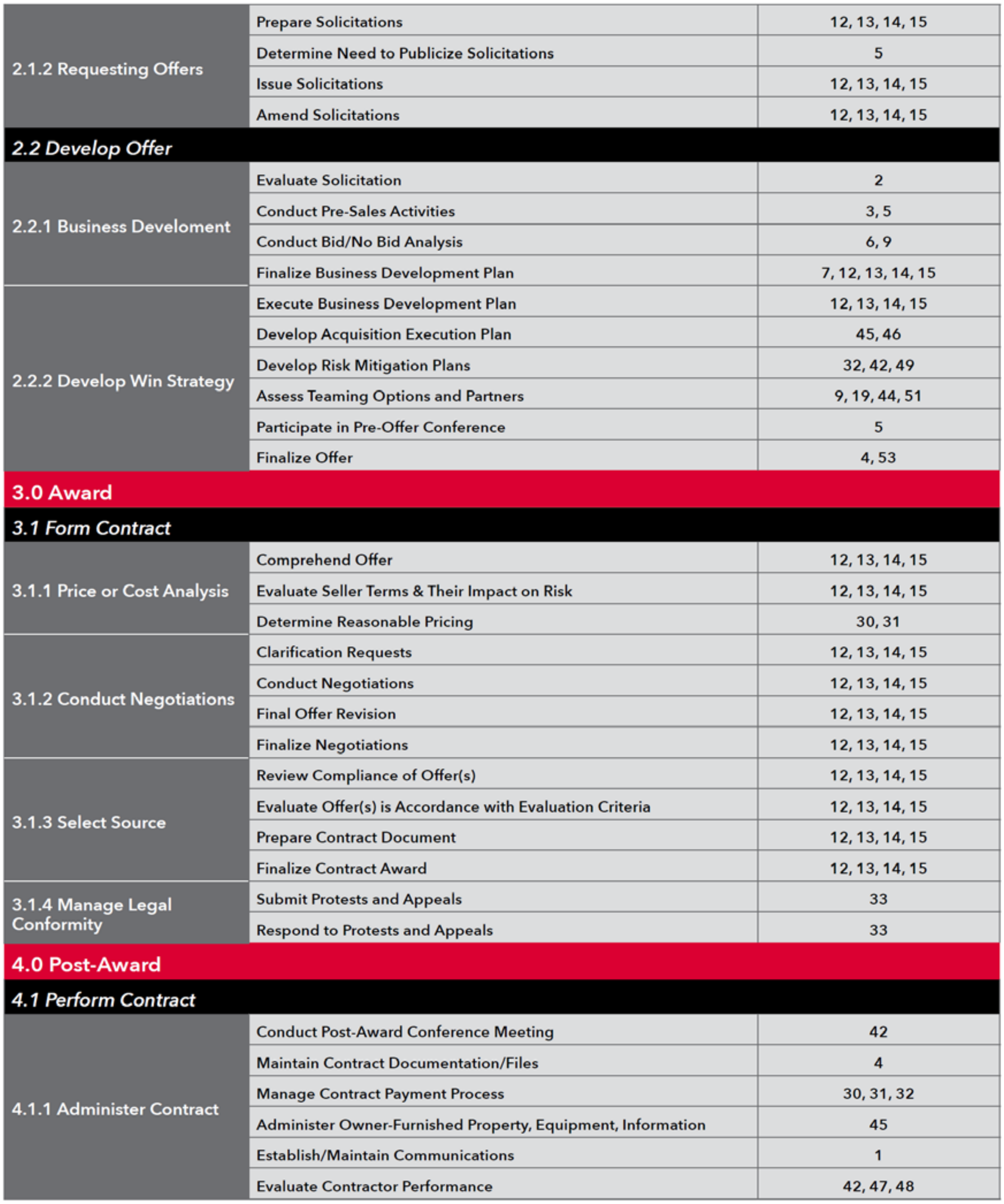


The *CMS-FAR* Matrix

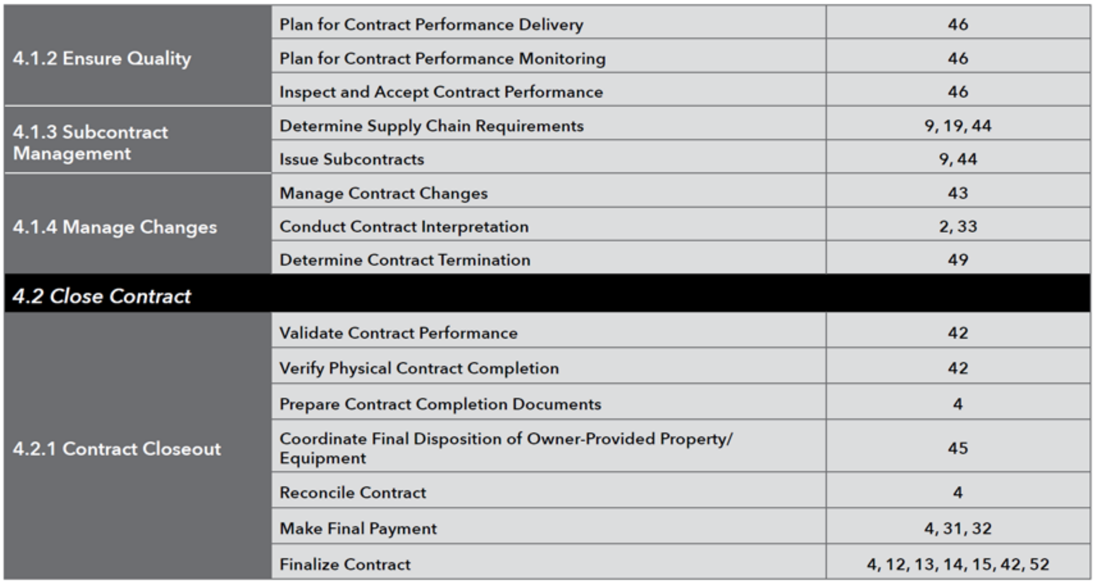
The following matrix cross-references the competencies of the *Contract Management Standard* (*CMS*) with the *Federal Acquisition Regulation* (*FAR*)

CMS COMPETENCY	JOB TASK	FAR PART
1.0 Guiding Principles		
1.1 Skills and Roles	Career Development, Contracting Authority, and Responsibility	1
1.2 Contract Principles	Statement of Guiding Principles for the FAR	1
1.3 Standards of Conduct	Improper Business Practices and Personal Conflicts of Interest	3
	Contractor Responsibility Standards	9
1.4 Regulatory Compliance	Application of Labor Laws to Government Acquisitions	22
	Environment, Energy and Water Efficiency, Renewable Energy Technology, Occupational Safety, and Drug-Free Workplace	23
	Protection of Privacy and Freedom of Information	24
	Manage Patents, Data, Copyrights, Bonds, Insurance, and Taxes	27, 28, 29
1.5 Situational Assessment	Special Contracting Methods	17
	Emergency Contracting	18
	Foreign Acquisition	25
	Major Systems Acquisition	34
	R&D Contracting	35
	Construction and A-E	36
	Service Contracting	37
	Federal Supply Schedule Contracting	38
	Acquisition of Information Technology	39
	Acquisition of Utility Services	41
	Extraordinary Contractual Actions and the Safety Act	50
1.6 Team Dynamics	Acquisition Team	1
	Definitions of Words and Terms	2
	Document Lessons Learned/Best Practices	4
2.0 Pre-Award		
2.1 Develop Solicitation		
2.1.1 Acquisition Planning	Perform Acquisition Planning	2, 7
	Shape Internal Customer Requirements	11
	Conduct Market Research	5, 10
	Identify Potential Suppliers	6, 8, 19, 26
	Evaluate Requirement Achievability	6
	Conduct Pre-Offer Conferences	10, 15
	Select Proper Contract Type	12, 13, 14, 15, 16
	Select Proper Contract Method	12, 13, 14, 15
	Determine Appropriate Business and Regulatory Requirements	12, 13, 14, 15
	Formulate Offer Evaluation Plan	12, 13, 14, 15

Note. Used by permission.



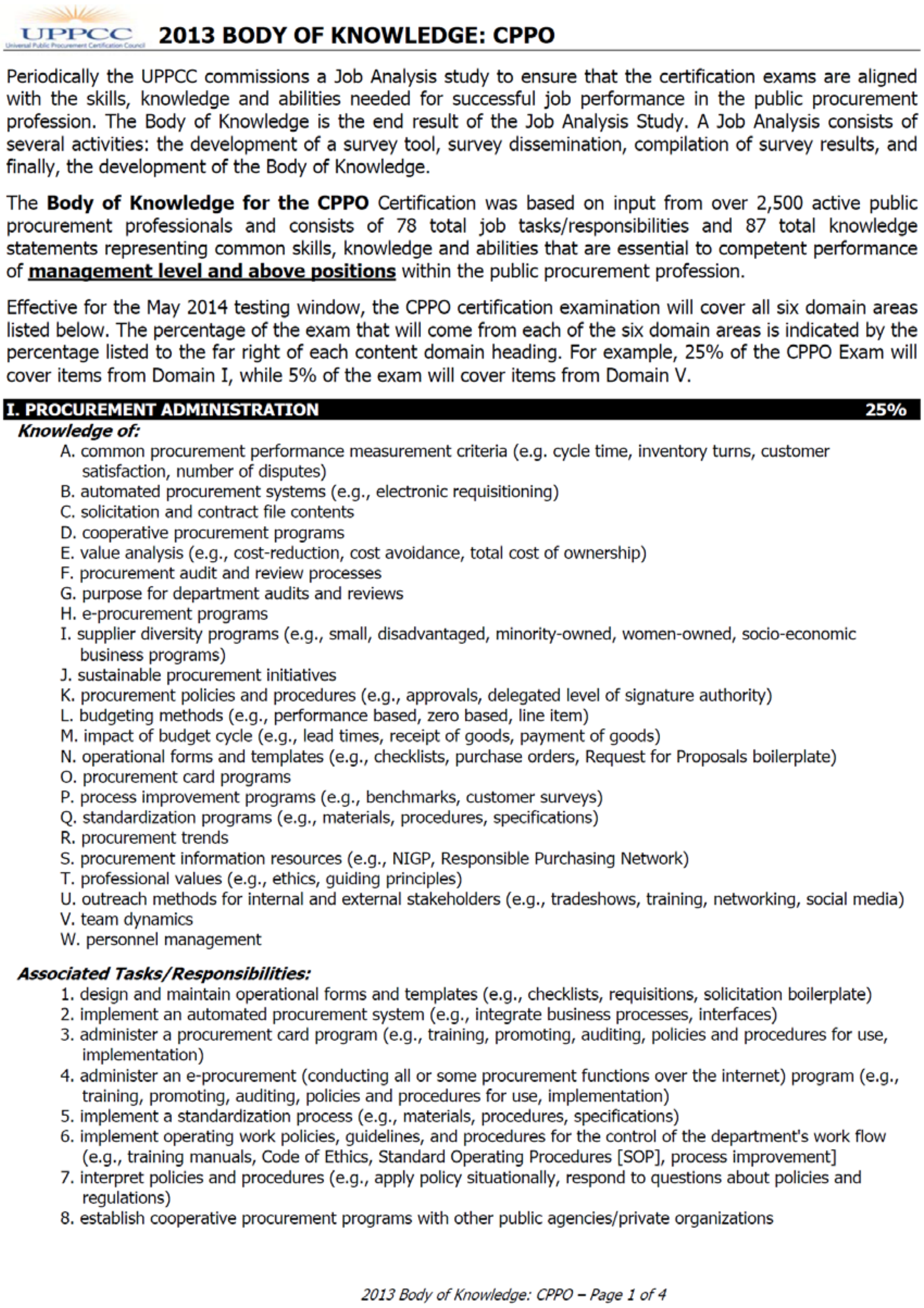
2.1.2 Requesting Offers	Prepare Solicitations	12, 13, 14, 15
	Determine Need to Publicize Solicitations	5
	Issue Solicitations	12, 13, 14, 15
	Amend Solicitations	12, 13, 14, 15
2.2 Develop Offer		
2.2.1 Business Develoment	Evaluate Solicitation	2
	Conduct Pre-Sales Activities	3, 5
	Conduct Bid/No Bid Analysis	6, 9
	Finalize Business Development Plan	7, 12, 13, 14, 15
2.2.2 Develop Win Strategy	Execute Business Development Plan	12, 13, 14, 15
	Develop Acquisition Execution Plan	45, 46
	Develop Risk Mitigation Plans	32, 42, 49
	Assess Teaming Options and Partners	9, 19, 44, 51
	Participate in Pre-Offer Conference	5
	Finalize Offer	4, 53
3.0 Award		
3.1 Form Contract		
3.1.1 Price or Cost Analysis	Comprehend Offer	12, 13, 14, 15
	Evaluate Seller Terms & Their Impact on Risk	12, 13, 14, 15
	Determine Reasonable Pricing	30, 31
3.1.2 Conduct Negotiations	Clarification Requests	12, 13, 14, 15
	Conduct Negotiations	12, 13, 14, 15
	Final Offer Revision	12, 13, 14, 15
	Finalize Negotiations	12, 13, 14, 15
3.1.3 Select Source	Review Compliance of Offer(s)	12, 13, 14, 15
	Evaluate Offer(s) is Accordance with Evaluation Criteria	12, 13, 14, 15
	Prepare Contract Document	12, 13, 14, 15
	Finalize Contract Award	12, 13, 14, 15
3.1.4 Manage Legal Conformity	Submit Protests and Appeals	33
	Respond to Protests and Appeals	33
4.0 Post-Award		
4.1 Perform Contract		
4.1.1 Administer Contract	Conduct Post-Award Conference Meeting	42
	Maintain Contract Documentation/Files	4
	Manage Contract Payment Process	30, 31, 32
	Administer Owner-Furnished Property, Equipment, Information	45
	Establish/Maintain Communications	1
	Evaluate Contractor Performance	42, 47, 48



4.1.2 Ensure Quality	Plan for Contract Performance Delivery	46
	Plan for Contract Performance Monitoring	46
	Inspect and Accept Contract Performance	46
4.1.3 Subcontract Management	Determine Supply Chain Requirements	9, 19, 44
	Issue Subcontracts	9, 44
4.1.4 Manage Changes	Manage Contract Changes	43
	Conduct Contract Interpretation	2, 33
	Determine Contract Termination	49
4.2 Close Contract		
4.2.1 Contract Closeout	Validate Contract Performance	42
	Verify Physical Contract Completion	42
	Prepare Contract Completion Documents	4
	Coordinate Final Disposition of Owner-Provided Property/ Equipment	45
	Reconcile Contract	4
	Make Final Payment	4, 31, 32
	Finalize Contract	4, 12, 13, 14, 15, 42, 52

Appendix E. UPPCC Body of Knowledge

(UPPCC, 2019)



UPPCC Universal Public Procurement Certification Council

2013 BODY OF KNOWLEDGE: CPPO

Periodically the UPPCC commissions a Job Analysis study to ensure that the certification exams are aligned with the skills, knowledge and abilities needed for successful job performance in the public procurement profession. The Body of Knowledge is the end result of the Job Analysis Study. A Job Analysis consists of several activities: the development of a survey tool, survey dissemination, compilation of survey results, and finally, the development of the Body of Knowledge.

The **Body of Knowledge for the CPPO** Certification was based on input from over 2,500 active public procurement professionals and consists of 78 total job tasks/responsibilities and 87 total knowledge statements representing common skills, knowledge and abilities that are essential to competent performance of **management level and above positions** within the public procurement profession.

Effective for the May 2014 testing window, the CPPO certification examination will cover all six domain areas listed below. The percentage of the exam that will come from each of the six domain areas is indicated by the percentage listed to the far right of each content domain heading. For example, 25% of the CPPO Exam will cover items from Domain I, while 5% of the exam will cover items from Domain V.

I. PROCUREMENT ADMINISTRATION 25%

Knowledge of:

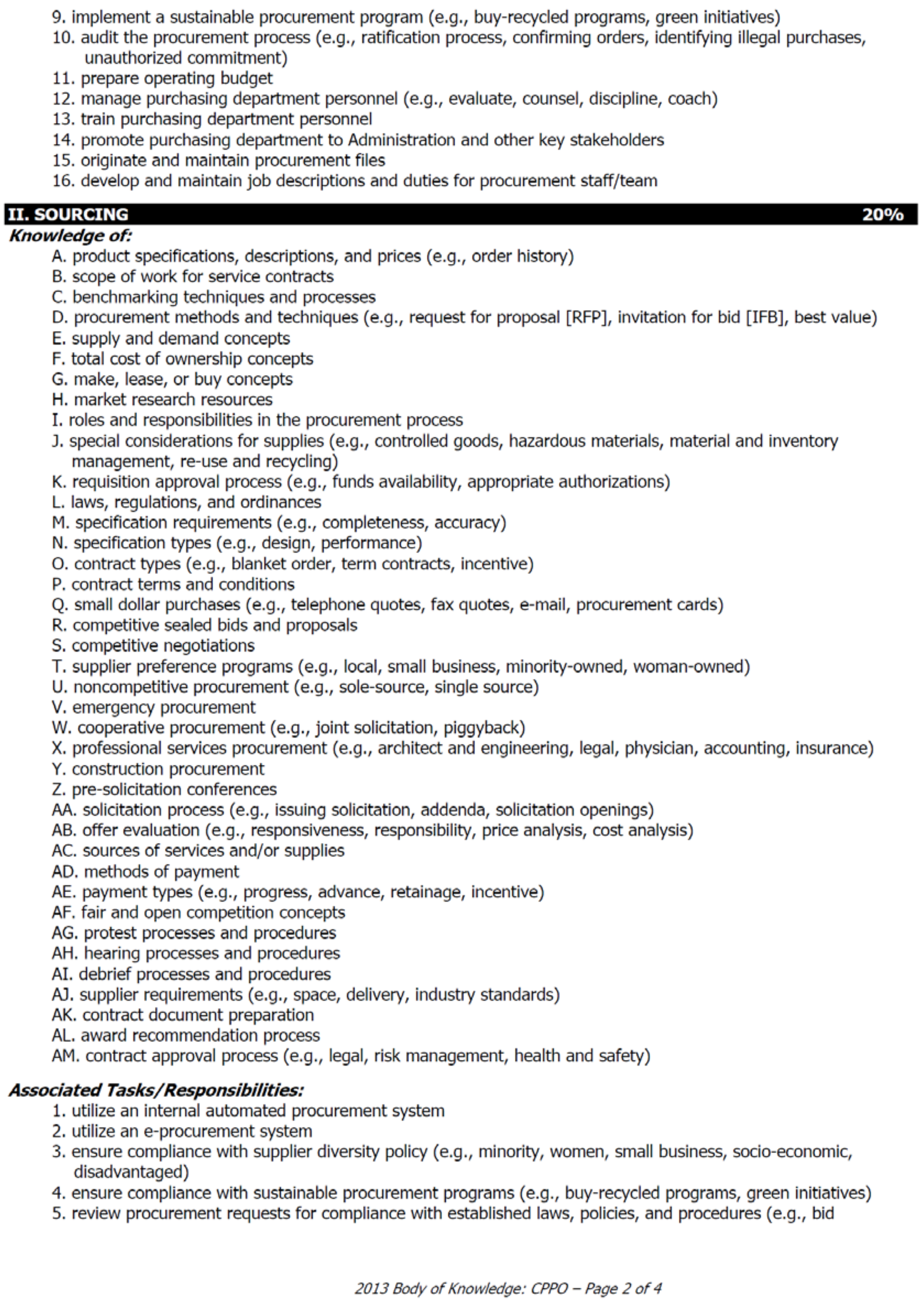
A. common procurement performance measurement criteria (e.g. cycle time, inventory turns, customer satisfaction, number of disputes)
B. automated procurement systems (e.g., electronic requisitioning)
C. solicitation and contract file contents
D. cooperative procurement programs
E. value analysis (e.g., cost-reduction, cost avoidance, total cost of ownership)
F. procurement audit and review processes
G. purpose for department audits and reviews
H. e-procurement programs
I. supplier diversity programs (e.g., small, disadvantaged, minority-owned, women-owned, socio-economic business programs)
J. sustainable procurement initiatives
K. procurement policies and procedures (e.g., approvals, delegated level of signature authority)
L. budgeting methods (e.g., performance based, zero based, line item)
M. impact of budget cycle (e.g., lead times, receipt of goods, payment of goods)
N. operational forms and templates (e.g., checklists, purchase orders, Request for Proposals boilerplate)
O. procurement card programs
P. process improvement programs (e.g., benchmarks, customer surveys)
Q. standardization programs (e.g., materials, procedures, specifications)
R. procurement trends
S. procurement information resources (e.g., NIGP, Responsible Purchasing Network)
T. professional values (e.g., ethics, guiding principles)
U. outreach methods for internal and external stakeholders (e.g., tradeshows, training, networking, social media)
V. team dynamics
W. personnel management

Associated Tasks/Responsibilities:

1. design and maintain operational forms and templates (e.g., checklists, requisitions, solicitation boilerplate)
2. implement an automated procurement system (e.g., integrate business processes, interfaces)
3. administer a procurement card program (e.g., training, promoting, auditing, policies and procedures for use, implementation)
4. administer an e-procurement (conducting all or some procurement functions over the internet) program (e.g., training, promoting, auditing, policies and procedures for use, implementation)
5. implement a standardization process (e.g., materials, procedures, specifications)
6. implement operating work policies, guidelines, and procedures for the control of the department's work flow (e.g., training manuals, Code of Ethics, Standard Operating Procedures [SOP], process improvement]
7. interpret policies and procedures (e.g., apply policy situationally, respond to questions about policies and regulations)
8. establish cooperative procurement programs with other public agencies/private organizations

2013 Body of Knowledge: CPPO – Page 1 of 4

Note. Used by permission.



9. implement a sustainable procurement program (e.g., buy-recycled programs, green initiatives)
10. audit the procurement process (e.g., ratification process, confirming orders, identifying illegal purchases, unauthorized commitment)
11. prepare operating budget
12. manage purchasing department personnel (e.g., evaluate, counsel, discipline, coach)
13. train purchasing department personnel
14. promote purchasing department to Administration and other key stakeholders
15. originate and maintain procurement files
16. develop and maintain job descriptions and duties for procurement staff/team

II. SOURCING **20%**

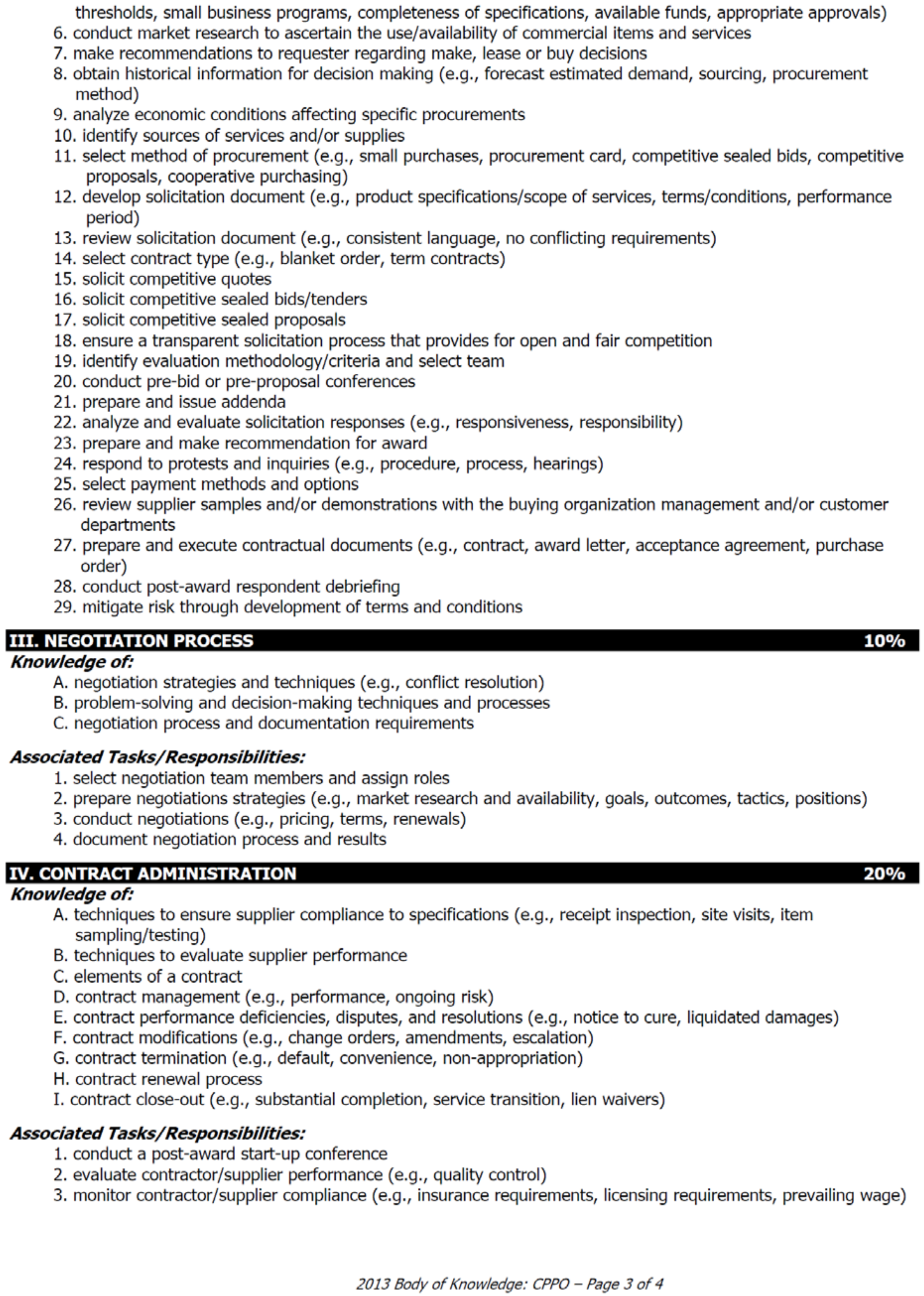
Knowledge of:

A. product specifications, descriptions, and prices (e.g., order history)
B. scope of work for service contracts
C. benchmarking techniques and processes
D. procurement methods and techniques (e.g., request for proposal [RFP], invitation for bid [IFB], best value)
E. supply and demand concepts
F. total cost of ownership concepts
G. make, lease, or buy concepts
H. market research resources
I. roles and responsibilities in the procurement process
J. special considerations for supplies (e.g., controlled goods, hazardous materials, material and inventory management, re-use and recycling)
K. requisition approval process (e.g., funds availability, appropriate authorizations)
L. laws, regulations, and ordinances
M. specification requirements (e.g., completeness, accuracy)
N. specification types (e.g., design, performance)
O. contract types (e.g., blanket order, term contracts, incentive)
P. contract terms and conditions
Q. small dollar purchases (e.g., telephone quotes, fax quotes, e-mail, procurement cards)
R. competitive sealed bids and proposals
S. competitive negotiations
T. supplier preference programs (e.g., local, small business, minority-owned, woman-owned)
U. noncompetitive procurement (e.g., sole-source, single source)
V. emergency procurement
W. cooperative procurement (e.g., joint solicitation, piggyback)
X. professional services procurement (e.g., architect and engineering, legal, physician, accounting, insurance)
Y. construction procurement
Z. pre-solicitation conferences
AA. solicitation process (e.g., issuing solicitation, addenda, solicitation openings)
AB. offer evaluation (e.g., responsiveness, responsibility, price analysis, cost analysis)
AC. sources of services and/or supplies
AD. methods of payment
AE. payment types (e.g., progress, advance, retainage, incentive)
AF. fair and open competition concepts
AG. protest processes and procedures
AH. hearing processes and procedures
AI. debrief processes and procedures
AJ. supplier requirements (e.g., space, delivery, industry standards)
AK. contract document preparation
AL. award recommendation process
AM. contract approval process (e.g., legal, risk management, health and safety)

Associated Tasks/Responsibilities:

1. utilize an internal automated procurement system
2. utilize an e-procurement system
3. ensure compliance with supplier diversity policy (e.g., minority, women, small business, socio-economic, disadvantaged)
4. ensure compliance with sustainable procurement programs (e.g., buy-recycled programs, green initiatives)
5. review procurement requests for compliance with established laws, policies, and procedures (e.g., bid

2013 Body of Knowledge: CPPO – Page 2 of 4



thresholds, small business programs, completeness of specifications, available funds, appropriate approvals)

6. conduct market research to ascertain the use/availability of commercial items and services
7. make recommendations to requester regarding make, lease or buy decisions
8. obtain historical information for decision making (e.g., forecast estimated demand, sourcing, procurement method)
9. analyze economic conditions affecting specific procurements
10. identify sources of services and/or supplies
11. select method of procurement (e.g., small purchases, procurement card, competitive sealed bids, competitive proposals, cooperative purchasing)
12. develop solicitation document (e.g., product specifications/scope of services, terms/conditions, performance period)
13. review solicitation document (e.g., consistent language, no conflicting requirements)
14. select contract type (e.g., blanket order, term contracts)
15. solicit competitive quotes
16. solicit competitive sealed bids/tenders
17. solicit competitive sealed proposals
18. ensure a transparent solicitation process that provides for open and fair competition
19. identify evaluation methodology/criteria and select team
20. conduct pre-bid or pre-proposal conferences
21. prepare and issue addenda
22. analyze and evaluate solicitation responses (e.g., responsiveness, responsibility)
23. prepare and make recommendation for award
24. respond to protests and inquiries (e.g., procedure, process, hearings)
25. select payment methods and options
26. review supplier samples and/or demonstrations with the buying organization management and/or customer departments
27. prepare and execute contractual documents (e.g., contract, award letter, acceptance agreement, purchase order)
28. conduct post-award respondent debriefing
29. mitigate risk through development of terms and conditions

III. NEGOTIATION PROCESS 10%

Knowledge of:

A. negotiation strategies and techniques (e.g., conflict resolution)
B. problem-solving and decision-making techniques and processes
C. negotiation process and documentation requirements

Associated Tasks/Responsibilities:

1. select negotiation team members and assign roles
2. prepare negotiations strategies (e.g., market research and availability, goals, outcomes, tactics, positions)
3. conduct negotiations (e.g., pricing, terms, renewals)
4. document negotiation process and results

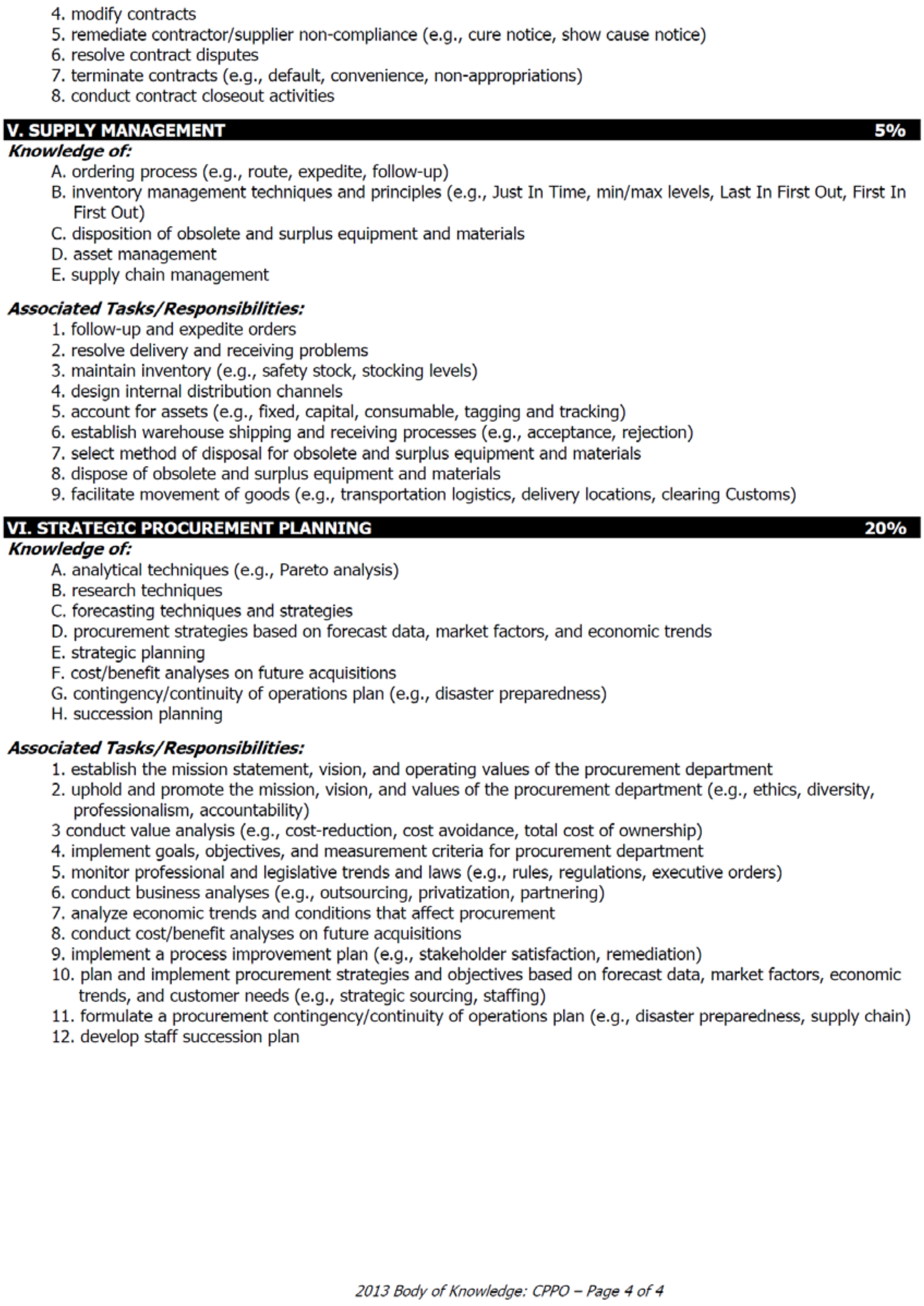
IV. CONTRACT ADMINISTRATION 20%

Knowledge of:

A. techniques to ensure supplier compliance to specifications (e.g., receipt inspection, site visits, item sampling/testing)
B. techniques to evaluate supplier performance
C. elements of a contract
D. contract management (e.g., performance, ongoing risk)
E. contract performance deficiencies, disputes, and resolutions (e.g., notice to cure, liquidated damages)
F. contract modifications (e.g., change orders, amendments, escalation)
G. contract termination (e.g., default, convenience, non-appropriation)
H. contract renewal process
I. contract close-out (e.g., substantial completion, service transition, lien waivers)

Associated Tasks/Responsibilities:

1. conduct a post-award start-up conference
2. evaluate contractor/supplier performance (e.g., quality control)
3. monitor contractor/supplier compliance (e.g., insurance requirements, licensing requirements, prevailing wage)



4. modify contracts
5. remediate contractor/supplier non-compliance (e.g., cure notice, show cause notice)
6. resolve contract disputes
7. terminate contracts (e.g., default, convenience, non-appropriations)
8. conduct contract closeout activities

V. SUPPLY MANAGEMENT 5%

Knowledge of:

A. ordering process (e.g., route, expedite, follow-up)

B. inventory management techniques and principles (e.g., Just In Time, min/max levels, Last In First Out, First In First Out)

C. disposition of obsolete and surplus equipment and materials

D. asset management

E. supply chain management

Associated Tasks/Responsibilities:

1. follow-up and expedite orders
2. resolve delivery and receiving problems
3. maintain inventory (e.g., safety stock, stocking levels)
4. design internal distribution channels
5. account for assets (e.g., fixed, capital, consumable, tagging and tracking)
6. establish warehouse shipping and receiving processes (e.g., acceptance, rejection)
7. select method of disposal for obsolete and surplus equipment and materials
8. dispose of obsolete and surplus equipment and materials
9. facilitate movement of goods (e.g., transportation logistics, delivery locations, clearing Customs)

VI. STRATEGIC PROCUREMENT PLANNING 20%

Knowledge of:

A. analytical techniques (e.g., Pareto analysis)

B. research techniques

C. forecasting techniques and strategies

D. procurement strategies based on forecast data, market factors, and economic trends

E. strategic planning

F. cost/benefit analyses on future acquisitions

G. contingency/continuity of operations plan (e.g., disaster preparedness)

H. succession planning

Associated Tasks/Responsibilities:

1. establish the mission statement, vision, and operating values of the procurement department

2. uphold and promote the mission, vision, and values of the procurement department (e.g., ethics, diversity, professionalism, accountability)

3 conduct value analysis (e.g., cost-reduction, cost avoidance, total cost of ownership)

4. implement goals, objectives, and measurement criteria for procurement department
5. monitor professional and legislative trends and laws (e.g., rules, regulations, executive orders)
6. conduct business analyses (e.g., outsourcing, privatization, partnering)
7. analyze economic trends and conditions that affect procurement
8. conduct cost/benefit analyses on future acquisitions
9. implement a process improvement plan (e.g., stakeholder satisfaction, remediation)
10. plan and implement procurement strategies and objectives based on forecast data, market factors, economic trends, and customer needs (e.g., strategic sourcing, staffing)
11. formulate a procurement contingency/continuity of operations plan (e.g., disaster preparedness, supply chain)
12. develop staff succession plan

2013 Body of Knowledge: CPPO – Page 4 of 4

Panel 5. Addressing Cybersecurity Within Defense Acquisition Programs

Wednesday, May 8, 2019	
12:45 p.m. – 2:00 p.m.	**Chair: Captain Kurt Rothenhaus, USN,** Navy's Tactical Networks Program Office (PMW 160) ***How Effectively Are DoD Weapon System Acquisitions Addressing Cybersecurity?*** Raj Chitikila, Government Accountability Office ***Acquisition Cybersecurity Management Framework*** Randy Maule, Naval Postgraduate School ***Cybersecurity: Converting Shock Into Action (Part 2)*** Robert Tremaine and Paul Shaw, Defense Acquisition University

Captain Kurt Rothenhaus, USN—Captain Rothenhaus assumed command of the Space and Naval Warfare Systems Center Pacific on 17 December 2013.

A native of New York City, Captain Rothenhaus received his commission after graduating from the University of South Carolina. He holds a Master of Science in Computer Science and a PhD in Software Engineering from the Naval Postgraduate School, and transferred into the Engineering Duty Officer community in 2003.

Captain Rothenhaus' operational assignments include USS FIFE (DD 991), USS O'BRIEN (DD 975), and Destroyer Squadron FIFTEEN, and he served as Combat Systems/C51 Officer on USS HARRY S. TRUMAN (CVN 75). Additionally, he served in Baghdad, Iraq, developing counter-insurgency and reconstruction systems for the Army Corps of Engineers.

His acquisition assignments include project manager at the Space and Naval Warfare Systems Center Pacific and various acquisition leadership roles in the Program Executive Office, Command, Control, Communications, Computers and Intelligence (PEO C41), to include Future Command and Control Systems Assistant Program Manager in the Navy Command and Control Program Office (PMW-150), and Assistant Program Manager for the Consolidated Afloat Network Enterprise System (CANES) in the Navy Tactical

Networks Program Office (PMW-160). Additionally, he served as the Deputy Program Manager for Navy Communications and GPS Program Office (PMW/A-170) from September 2011 to October 2013.

Captain Rothenhaus received the A. Byran Laswell, National Defense Industrial Association Award in 2007 for technology innovation and was a 2008 Navy & Marine Corps Leadership Award winner while serving aboard USS HARRY S. TRUMAN (CVN 75). His personal awards include the Meritorious Service Medal, Joint and Navy Commendation Medal, Navy Achievement medals and various service and campaign awards.

Acquisition Cybersecurity Management Framework

Dr. Randy William Maule—has been with the Naval Postgraduate School since 2000, serving as naval and joint forces enterprise developer, knowledge manager, and technical analyst in Sea Trial and coalition exercises where he conducted systems test and measurement. His enterprise tool suite and cyber test and measurement architecture operated on ships, in maritime and network operations centers, and in forward-deployed commands for nearly 15 years. Prior to this, he spent 10 years in Silicon Valley high technology industries researching intelligent networks and service architecture, and prior to this developing enterprise knowledge systems and artificial intelligence (AI) at a federal supercomputer center. [rwmaule@nps.edu]

Abstract

Current organizational structures have proven insufficient for cyber and information assurance. The acquisition role may be resourced and expanded to support information assurance and systems compliance. A supply chain audit and assessment process within acquisition departments will better support emerging cybersecurity requirements. This project advances technical and workflow models, an assessment framework, and implementation methods to support expansion of the acquisition department role to include cybersecurity and information assurance across the systems lifecycle—from supply chain, through test and measurement, to maintenance and obsolescence. Analysis methodology and model-based system engineering techniques successfully employed in naval and joint forces field research for technology and cybersecurity evaluation for nearly two decades, along with best practices from Silicon Valley high technology industries, were applied in the acquisition cybersecurity management framework. A shift of cybersecurity assessment from distributed units into centralized acquisition departments should significantly lessen the inter- and intra-organizational boundaries which have traditionally hindered cybersecurity.

Research Objective: Establish methodology and models to support the cybersecurity and information assurance needs of naval forces and provide decision makers with an evaluation framework and workflow to inform acquisition decisions and better ensure systems security.

Research Questions: Will the centralization of cybersecurity and information assurance away from individual units into acquisition departments lessen inter- and intra-organizational boundaries that have historically limited cyber effectiveness? Will the workflow and audit models suffice for acquisition departments to implement security controls across the systems lifecycle—from initial acquisition to maintenance and obsolescence?

Introduction

Current organizational structures have proven insufficient for cyber and information assurance. Acquisition departments may be expanded to help ensure cybersecurity. This research advances the acquisition role to support information assurance throughout the supply chain and across the lifecycle of the equipment. This is proposed as an enhancement to current acquisition processes. Model-based system engineering techniques are applied for systems test and measurement and integrated into audit processes within the acquisition workflow. Techniques, procedures, roles and responsibilities are based on lessons learned in naval and joint forces exercises and best practices in Silicon Valley high technology industries. The proposed supply chain audit and assessment process extends from initial equipment purchase order, through acquisition, to maintenance and lifecycle compliance assessment, to obsolescence and destruction.

Research Background

Business, industry, and government collectively struggle with cybersecurity compliance, information assurance, and data security. Resources and processes to support audits, assessment and reporting are insufficient. While the terminology and architecture are slightly different from industry to government, the problems are similar and can often be traced to the supply chain—from counterfeit and compromised components, to improper/malevolent code, to unsecured systems and maintenance processes. The acquisition role may be best suited to remedy current shortcomings. This will require significant expansion of that role and its resources to support supply chain information assurance.

Cybersecurity compliance assessment as a component of supply chain management will shift audit responsibilities from vendors, program offices and departments into centralized acquisition departments. This will significantly lessen the inter- and intra-organizational boundaries which have traditionally hindered cybersecurity and information assurance. The shift of systems verification from vendors and their contractors or sponsors to independent government auditors will remove bias while increasing the comprehensiveness of the process as auditors are able to look across department boundaries to examine the integration interfaces where systems are most vulnerable. Model-Based System Engineering (MBSE) and supporting analysis methodology successfully employed in naval and joint forces field research for technology and cybersecurity evaluation for nearly two decades provide the foundation for the acquisition modeling framework and analysis workflow.

The process begins with technical models and expert systems for best practices, then procedures and workflows for technical assessment, followed by systems integration audits. Next are methods and procedures for in-service audits for cybersecurity and information assurance, systems verification and data validation. Technical models are integrated with audit workflows for comprehensive lifecycle systems assessment to include maintenance and the declaration of software/hardware obsolescence and destruction.

Literature Review

Supply chain modeling and analysis is advanced within the context of complexity science, which assumes both technical and human phenomena that interface to determine system readiness and operational effectiveness. The following is evidence of complexity in naval systems:

1. Multi-layered communication architecture
2. Multiple organizational structures to produce a capability
3. Organizational boundaries which impact engineering and analysis
4. Adversary capabilities for advanced electronic and multi-layered cyberattack.

The methodology herein advances multi-disciplinary research techniques to include evaluation of all variables that we have found to impact the validity of naval systems and data, including cross-organizational technology integration, variance in the RF spectrum, and human influence (Maule, 2017). There is a research history that provides perspective for supply chain cyber analytics.

Network science studies complex networks (Tiropanis et al., 2015) at a level of detail sufficient to generate predictive models. For example, tools that we use in naval technical analysis map data flows between systems over network connections to monitor routing, processes and data. Supporting each variable are algorithms to assess defined metrics and data validity based on components in the routing, integration and transformation path.

Network-centric warfare and information dominance are considered within the vocabulary of network science (National Research Council, 2005). When cybersecurity is layered into the analysis, the number of metrics for measurement expands exponentially.

Complexity science spans computer science, mathematics, and operations research and includes the study of distributed, interactive computing (Du & Ko, 2014). Complexity theory investigates how subcomponents of a system integrate to produce a collective behavior of that system (Ladyman, Lambert, & Wiesner, 2013). Pertinent to naval systems analysis is that complexity can be characterized within the context of equilibrium—as required for high-performance communications in challenged environments. Absent system synchronization, we do not achieve equilibrium, so data relied upon for decisions may be latent, corrupt or compromised. A sub-discipline of complexity science, adaptive systems, uses probabilistic measures to quantify complex variables—such as systems readiness and human effectiveness.

Adaptive systems are characterized by the capability to change and learn from experience. Machine learning can be applied to help understand the complexity. We observe adaptive behaviors in naval exercises as we instrument networks to monitor complex data flows across geographic regions. The components of systems interact, with the result of those interactions dependent on dynamic contextual variables. An example is changes made as sailors and systems adapt to rapidly changing tactical scenarios. Evaluation addresses the dynamic interplay of adaptive, complex variables over time. Failure to address this complexity results in an inability to monitor systems to recognize a performance variance or cyber intrusion, or to adapt the analysis to changes in systems operational context—leading to incorrect data.

Test and measurement of naval systems in live operations have established that the relationship between systems, components, and other systems is nonlinear (Maule, Jensen, & Gallup, 2014). It is not possible to precisely define the inputs such that there is a direct relationship to the outputs. Cause–effect relationships can be determined only within technical, operational and environmental context. Systems performance tends to exhibit divergent patterns under stress—such as challenged communications, jamming or electronic attack, and of course cyber manipulation.

This leads to the final construct of adaptive complexity—namely, that while it is possible to establish linear relationships in a static architecture, these relationships may no longer be relevant when integrated into dynamic scenarios. Researchers have noted the need for probabilistic algorithms for multiple dimensions of analysis when contexts are dynamic and expanding (McMullen, 2015). Assessment is over time, within the full range of technical, operational and environmental contexts in which the system will operate (Maule, 2016).

Probabilistic algorithms also fit nicely with artificial intelligence (AI) tools for decision support. In warfare, the large number of dynamic variables, together with the large number of possible technical, operational and environmental contexts to be assessed in an engagement, necessitate statistical analysis. There is never a single answer; the result is always within context. Probabilistic approaches, together with machine learning and neural networks, can address this complexity to provide a solution for tactical supply chain cyber analysis.

The need is acute. Problems with unsecured open architecture and open source products persist (Dorofee et al., 2013; Cooper, 2009; Lindqvist & Jonsson, 1998). There are problems when vendors publish system specifications to the Internet and problems with deployment practices that do not carefully control firmware updates (Kern, 2014; Camp et al., 2006). There is little protection if purchasing computer chips which have already been compromised (Center for Public Integrity, 2014; Rossi, 2012; Johnson, 2011; Adee, 2008; Grow et al., 2008; Dean & Li, 2002).

Another rationale for a direct connection between the audit process and the acquisition role is so that compromised systems can be immediately destroyed and replaced. Historically, after we identify a breach, we can only file a report. These reports are not typically well-received, and systems may continue to operate. In the proposed supply chain cybersecurity workflow, the auditors have a more direct means for remediation.

As needed, events can be reconstructed for detailed cyber analysis. We use live cyberattacks on components in offline laboratories to validate findings. The analytics produce quantitative system readiness coefficients and confidence levels for those coefficients (Maule, 2017).

Method

Adaptive complexity for supply chain cyber analysis is applied as an extension of the Cybersecurity Figure of Merit (CFOM). CFOM is a mathematical framework of weighted qualitative and quantitative metrics that provide an expression of the relative effectiveness of an information technology in terms of the completeness and sufficiency of its cyber security properties throughout its lifecycle (Space and Naval Warfare Systems Command [SPAWAR], 2015).

The NPS Service Evaluation Architecture (SEA) CFOM implementation is based on assessments conducted in live naval, joint forces and coalition exercises where the focus was on systems readiness and resiliency in electronic engagements against adversaries that had imposed D-DIL or A2AD conditions on blue forces (Maule & Lewis, 2011).

Models, metrics, and analytics are derived from cumulative naval system test results, beginning with Fleet Battle Experiments in 2000 and then FORCEnet and Joint Forces Command (JFCOM) Sea Trials from 2003–2015, which included Trident Warrior, RIMPAC, Valiant Shield, and numerous limited objective experiments with NATO and coalition forces.

Supply Chain Standards

Next is to address foundations for the supply chain cybersecurity framework to help structure the analysis. The International Organization for Standardization (ISO) is a global network of national standards bodies which develop and publish International Standards. Members are the foremost standards organizations in their countries. The ISO collaborates closely with the International Electrotechnical Commission (IEC) and the Institute for Electrical and Electronics Engineers (IEEE). Some of the standards are specific to supply chain management, including cybersecurity, quality management, and audits (ISO, n.d.). Standards pertinent to the acquisition cybersecurity management framework include the following:

- SO 9000: Quality management systems
- ISO/TS 10303-1307: Industrial automation systems and integration
- ISO 16678: Guidelines to deter counterfeiting and illicit trade
- ISO/TR 17370: Data carriers for supply chain management

- ISO/IEC 20243: Mitigating maliciously tainted and counterfeit products[1]
- ISO/TS 22375: Security and resilience guidelines for complexity assessment
- ISO/IEC 27036: Information security for supplier relationships
- ISO 28000: Supply chain security management systems—Specifications
- ISO 28001: Supply chain security management systems—Assessments
- ISO 28002: Supply chain security management systems—Resilience
- ISO 28003: Supply chain security management systems—Audit and certification
- ISO/IEC/IEEE 41062: Software engineering

Supply Chain Acquisition Framework

The acquisition cybersecurity management framework and supply chain cyber analytics process apply the previously mentioned standards through an extension to the traditional acquisition workflow. The extension provides cybersecurity management from initial equipment request through vendor selection, then across the systems lifecycle to include maintenance and obsolescence. The intent is to provide a comprehensive security structure for naval systems from acquisition to destruction (Figure 1). This includes the system support structure and command management, staffing, contracting and outsourcing. Time requirements along with expertise, budgeting and comparative analysis are addressed.

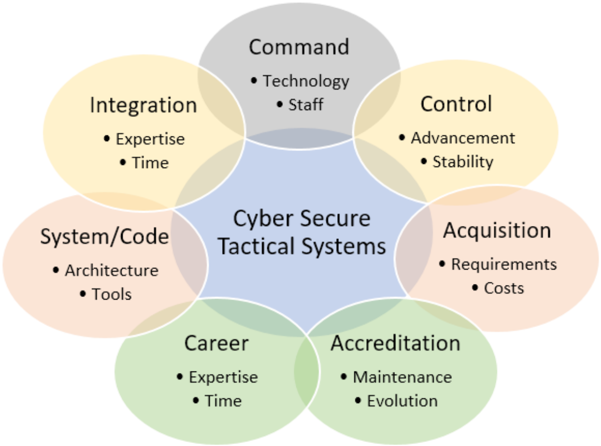


Figure 1. **Variables for Supply Chain Cyber Assessment**

Evaluation techniques are based in statistical analysis with AI and machine learning to provide decision support. Probabilities are based on defined metrics and measurements from independent government auditors. The methodology can be applied to help acquisition decision makers better evaluate technologies for possible cybersecurity impact and tactical forces to better understand the implications of their purchase requests, the degree to which their systems may have been compromised, and the validity of the data in their systems.

[1] https://www.iso.org/standard/74399.html; https://www.iso.org/obp/ui/#iso:std:iso-iec:20243:-1:ed-1:v1:en

The assumption herein is that when naval architecture is suspected of compromise and the cyber adversary may have enacted automated routines to alter data to impact systems performance or invalidate information in command decision systems, mechanisms will be required to determine the impact on warfighter readiness. The proposed enhancement to the systems acquisition process will help remedy this situation through real-time audit monitors and controls.

Figure 2 denotes the basic acquisition process and the current financial and vendor selection process. Along the left axis is equipment selection and the purchase request. The green arrows indicate legacy operations. Below the basic acquisition process is the proposed cybersecurity enhanced acquisition process. Red arrows denote the additional workflows and data streams.

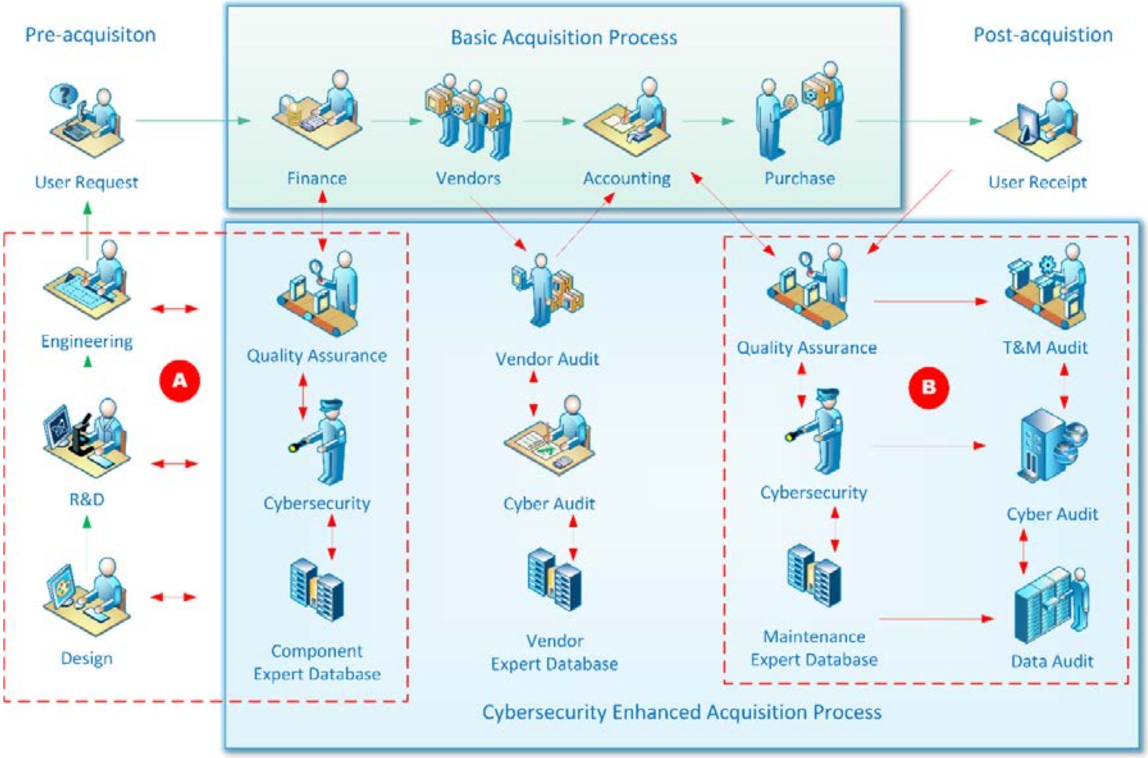


Figure 2. **Supply Chain Basic and Cybersecurity Enhanced Acquisition Framework**

Within the enhanced process are databases for quality assurance and cybersecurity, along with expert systems to interface with engineers during design and development—preliminary to product request and submission to the purchasing agents. The green arrows indicate the current workflows, and the red arrows are the interfaces to the new specialized systems.

The dashed red box designated as Section “A” is preliminary to the acquisition when the system proponent begins the purchase order. Here the purchaser interacts with expert systems as machine learning agents assess the technology through comparative analysis and provide recommendations. A record stream for acquisition decision makers and financial personnel is generated. Functions in this area are discussed in the solution section later in this report.

The dashed red box designated as Section "B" is the post-purchase process and consists of a series of independent government monitors and audits. Most can be automated and have been successfully tested in naval operations. These monitors and audits recognize that the purchase is not the end of the acquisition process, but rather a step in the systems lifecycle. Before the purchase, the cybersecurity concerns are with the computer chips and embedded components, drivers and software. After the purchase, the cybersecurity concerns are with the integration, maintenance and evolution of the software and components within the system, impact on other systems, and the validity of the processed data. Functions in this area are advanced in more detail in the next section and are discussed again in the solution set later in this report.

The unbound area in the middle of the figure addresses the physical components—from the vendor, to the suppliers to the vendor, to the involved personnel. This is a comprehensive area for assessment that is beyond the scope of this project and is reserved for future research. Techniques advanced in Sections "A" and "B" can be applied, albeit with an exponential expansion of detail and complexity.

Supply Chain Audit Framework

The audit framework begins with test and measurement models that show components, systems, spectrum, interfaces, sensors and software. All are assessed within the technical, operational and environmental context in which they operate to provide a more accurate analysis for acquisition decision makers. Collected data includes packets, system logs, sensor data, human interface and interaction results, and fusion/integration artifacts (Figure 3).

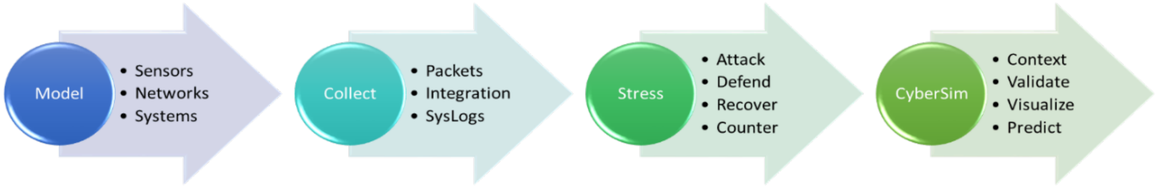


Figure 3. **High Level Supply Chain Cyber Audit Workflow**

Analysis of cyber effects begins with stressing systems through network and process load to determine points of failure and countermeasures to achieve resilience. Cyber effects are layered to assess system capabilities to recover from and/or counter cyber stress. Assessment involves a continuous, comprehensive monitoring of systems, networks and applications. CyberSim is for offline tests with live malware against the components to provide a more accurate cybersecurity assessment for systems verification and data validity. This data feeds the AI routines for algorithmic prediction of systems operational readiness.

In more detail, the supply chain cyber audit framework (Figure 4) supports in-service test and measurement for continuous systems cybersecurity assessment–using many of the same techniques successfully implemented on forward-deployed ships and in network and maritime operations centers in Sea Trials and coalition exercises. Our audits include not only new innovations but also updates to program of record systems.

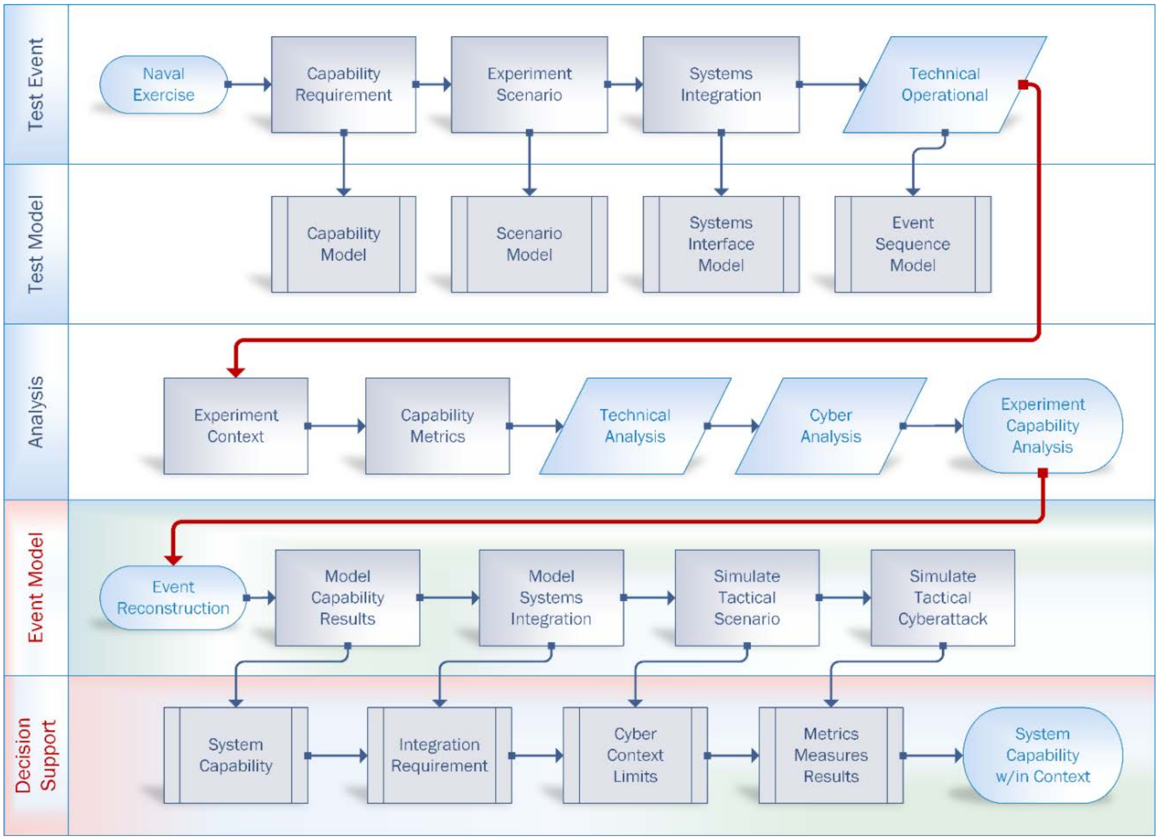


Figure 4. **Supply Chain Technical Analysis Framework and Workflow**

Cyber analytics is conceptualized as a continuing flow of tests across the operational lifecycle of a system. Each operational context, test scenario, vignette, and attack advance the machine learning algorithms and predictive capability of the audit models. In the previous example, the analysis is focused on ships in A2AD and communication-challenged environments. Systems are under electronic attack—our typical live event scenario throughout the Sea Trials.

The audit workflow starts with Department of Defense Architecture Framework (DoDAF) models of the system, for which at-rest baselines are established. Systems are then evaluated against these models in at-sea tests with active jamming and cyber/electronic attack. Communications between components/sensors require evaluation of satellite communications, tactical radios, and airborne over-the-horizon capabilities.

Cyberattacks are analyzed for their results on the acquisition component, including system failures, data corruption or manipulation, and degradation of situational awareness of supported command decision systems. Cyber performance and operational measures update or verify models and validate the quality of the data. The process iterates.

Solution

This section applies the previously discussed acquisition framework and analytics process as an extension of a traditional systems lifecycle to provide structure for naval systems supply chain cyber analysis.

Integration DEFinition (IDEF) models are common in the DoD to represent operations (IDEF, n.d.). Like DoDAF, the IDEF models range from high-level functional models to low-level object-oriented design and simulation. For a supply chain analytics workflow, the IDEF modeling approach provides useful operational representations in addition to precise data/information metrics for decision support.

The solution set integrates the previously discussed supply chain framework and workflow (pre- and post-acquisition) with implementation constructs for systems verification and data validation through the addition of

a. Experts and expert systems to the pre-acquisition engineering processes
b. Independent audits for information assurance and systems verification
c. Machine learning for AI support to supply chain decision makers

Core processes (Figure 5) include IDEF0 inputs, outputs, controls and mechanisms plus additional audit and AI layers. Core inputs are the purchase order and budget; outputs are the purchase and supporting maintenance agreements. Controls address guidelines and approvals required for submitters and purchasing agents. Mechanisms include the system, software or component requirements and specifications.

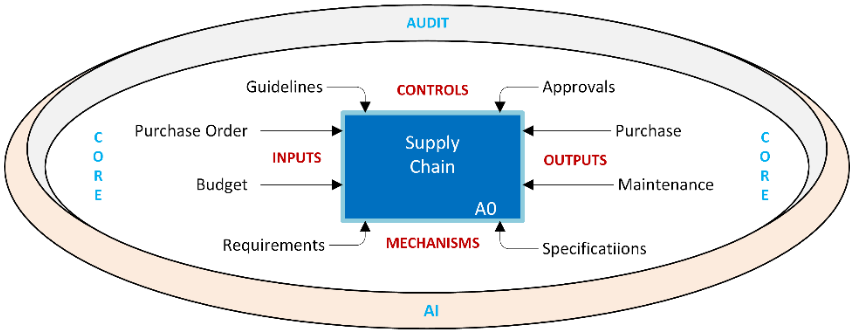


Figure 5. **IDEF A0 High-Level Solution Framework**

Core Workflow

Figure 6 presents IDEF steps A1–A5 as the high-level components of the supply chain cybersecurity workflow. Assessment begins with user requirements and controls to determine whether specifications have adequately addressed technical, operational and environmental variables that impact the integrity of the equipment in its intended operations.

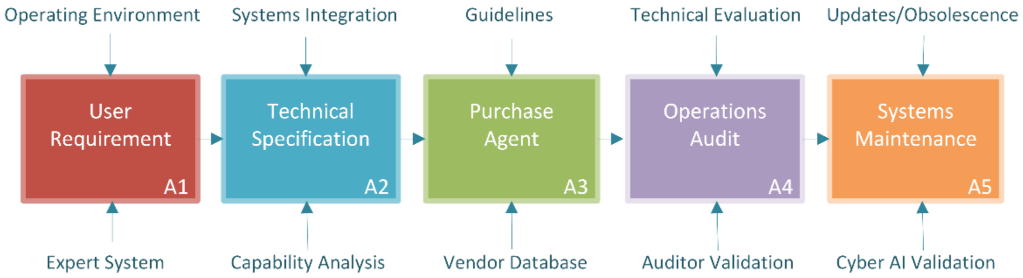


Figure 6. **Core Workflow for Supply Chain Cybersecurity Integrity Analysis**

Next are technical specifications with systems integration controls. This becomes a primary data set for the machine learning algorithms to address process conflict or constrained environments and will be one of the more extensive programming efforts due to the number of variables in a complex and dynamic naval architecture.

In operation, the purchasing agent receives the recommendation from the machine learning output and is simultaneously presented with the option to review the specific criteria upon which the recommendation is based. Controls include restrictions specific to the unit.

Upon receipt of the system (hardware, software, service, etc.) the responsibility for verification and validation shifts to the auditor. Upon auditor approval, the system is transferred to the end user.

Finally, the maintenance phase monitors equipment throughout its lifecycle, including patches and updates, until the declaration of obsolescence and verification of destruction. Important is the means to verify that the system or software has been destroyed due to the cyber risk from unsupported components.

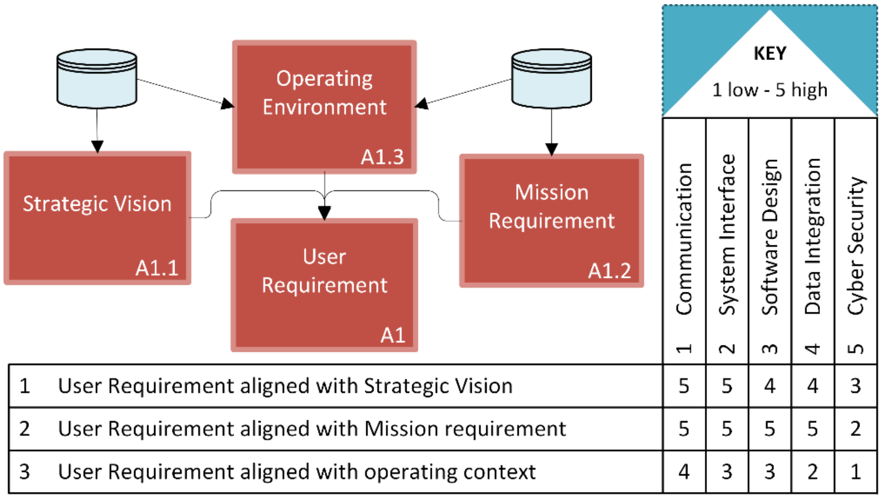
The next two sections examine A1 and A2 in more detail (A3–A5 are reserved for future research). In Figure 2, both are represented in the initial block "A" which occurs prior to the purchase. In future research, the approach followed for the technical specifications will also be applied in the operations audit (A4) and maintenance (A5) phases—albeit with the addition of metrics for technical, operational and environmental context to address the added complexity of live operations.

Requirement Audit

Audits are key to integrity validation across the supply chain. Auditors need to be properly trained and equipped, and with the capability to act independently without fear of reprisal. Nor should they have a vested interest in the success or failure of the system. All are common problems we encounter in analysis.

In Section "A" (Figure 2), with enough audits and a supporting database of audit results, the requirements review can be automated such that the purchaser interacts with an expert system and AI agents provide feedback and recommendations.

Figure 7 models the process and breaks out the Quality of Service (QoS) variables, metrics for those variables, and ratings key. Variables include (1) alignment with the strategic vision, (2) alignment with the mission statement, and (3) alignment with the operating environment. These variables can be programmed into an expert system.



		1 Communication	2 System Interface	3 Software Design	4 Data Integration	5 Cyber Security
1	User Requirement aligned with Strategic Vision	5	5	4	4	3
2	User Requirement aligned with Mission requirement	5	5	5	5	2
3	User Requirement aligned with operating context	4	3	3	2	1

Figure 7. **User Requirement Initial Audit Phase With Metrics and Ratings**

More difficult are the metrics and ratings which require in-depth understanding of the components of the system and the complexities of the operating environment and software. A typical approach is to begin analysis with the user's requirements for communications to assess alignment with the vision and mission, then the specifics of the operating context, including the organizational, technical and environmental conditions in which the equipment will operate.

The system interface metric examines innovation integration with components of the strategic plan, and then the specific mission area(s) in which it will operate. The context addresses interfaces to technical, operational and environmental conditions but at a deeper level. Technical context addresses the specifics of the physical interface—an area for further refinement and additional audit layers in future research. The environmental context categorizes the innovation through physical presence—for example, mobile device versus server, ship versus shore deployment, calm seas versus challenged communications. The operational baseline establishes whether the test is static or dynamic within the specifics of the test scenario. This area will also require much deeper analysis in future research.

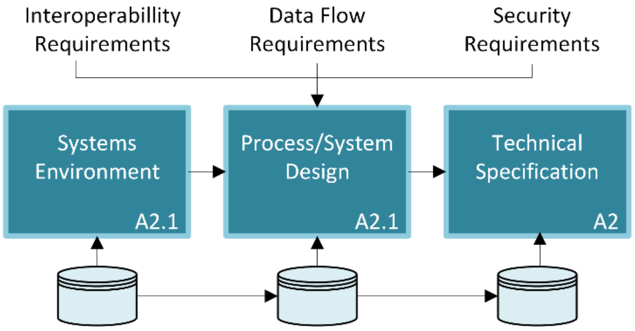
Software design is more straightforward and looks at the innovation in the context of currently active capabilities. For example, is this a redundant capability? Is the system rated by one of the major laboratories? Is this to be purchased? Developed in-house? Outsourced?

In a similar vein, data integration addresses the alignment of the innovation with the vision, mission, and end state: Will data be merged? Will this capability build on the output of another device? Create new insight? QoS variables are addressed from a command decision perspective.

Finally, the cybersecurity. Too often this is an after-thought, but this placement in the initial audit helps ensure that cybersecurity is at the forefront of the supply chain assessment workflow and aligned with the vision, mission and operating context. A2, below, adds more detail and addresses the actual engineering technical measurement process.

Specification Audit

The A2 technical audit identifies specifics within the systems environment, looking at system/service/process integration and interfaces (Figure 8). The first QoS variable assesses alignment of the technical specifications with the designated systems environment in which the equipment will operate to establish baselines. Until baselines are established, it may be difficult to discern a performance anomaly or cyber intrusion.


Interoperabillity Requirements
Data Flow Requirements
Security Requirements
Systems Environment A2.1
Process/System Design A2.1
Technical Specification A2

KEY
1 low - 5 high

		1 Systems / Nodes	2 Service Interfaces	3 Interoperability	4 Data Integration	5 Cyber Security
1	Technical specifications address operational environment	5				2
2	Technical specifications address systems environment	4	4			4
3	Technical specifications address system integration	4		3	2	2
4	Technical specifications address data, processes and services	4	4	4	2	4
5	Architecture details operations within context (OV-1)	4				2
6	Architecture details systems interfaces (SV-1)	5	5			2
7	Architecture details systems integration (SV-2)	4		4	2	4
8	Architecture details data and service, process flows (OV-6c)	4	3	3	2	2

Figure 8. **Technical Specification and Architecture Audit Phase, Metrics and Ratings**

Performance, interoperability, and integration metrics are assessed for (a) the technology, (b) the technology within the operating environment, (c) interaction of the technology with the other systems in that environment, and (d) the technology under full operational load from all systems in the environment in a cyber/electronic warfare engagement. Process and data flows are assessed, as is the cybersecurity of the system for each process and data flow.

Systems integration functions are similarly evaluated for performance, interoperability, and integration. This step examines the impact of other systems on the equipment and the impact of the new equipment on the existing configuration. Data and process flows are examined at the interface level.

The auditors assign weights/ratings to the tests, and these data populate training databases for machine learning. AI helps the decision makers understand the findings while reducing the complexity of the audit metrics.

Conclusion

Supply chain integrity analysis requires assessment of a complex mix of dynamic and adaptive variables. Systems lifecycle evaluation includes not only the equipment being tested, but also the impact of the collective enterprise, interplay of hosting networks and intervening systems, and remote data processes. Measurements are against metrics derived from models and their variables—prior to acquisition for alignment and post-acquisition for in-service analysis. The method advanced in this report provides a technique to evaluate supply chains to address variables that impact systems integrity and a workflow for in-service auditing and assessment.

Initial levels of analysis were presented, with examples for high-level audit variables, their metrics, and measurement methods. The research addresses the problem of engineering practices which do not adequately address cybersecurity, information assurance, and data validity over the lifecycle of a system. The method, framework and techniques were active for 15 years on ships, in network operations and fusion centers, and in deployed shore facilities to assess naval and joint forces technologies. This included field tests of over 500 complex systems-of-systems innovations in live operations. Through this research, the supply chain problems became readily apparent. Techniques advanced herein were proven to verify systems and validate data.

The approach layers independent audits with information assurance and cybersecurity as facets of quality management and associated performance controls. Audit layers were presented as enhancements to the basic acquisition process. Separation of assessment into an independent unit reporting to acquisition departments will help avoid entanglements that impact auditors in naval systems analysis.

To evaluate the framework and workflow, a proof-of-concept will be developed. AI and multi-database capabilities will be presented in the final report. In future research, AI may be further applied to help with supply chain decisions and ensure systems integrity. Preliminary tests with weights for the machine learning algorithms seem promising and worthy of development. For acquisition personnel, the AI prediction capabilities for equipment viability based on specifications and previous test results seem promising. Development of machine learning processes into repeatable formal methods is an additional area for future research.

References

Adee, S. (2008). The hunt for the kill switch: Are chip makers building electronic trapdoors in key military hardware? *IEEE Spectrum*. Retrieved from http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch

Camp, L., Goodman, S., House, C., Jack, W., Ramer, R., & Stella, M. (2006). Offshoring risks and exposures. In W. Aspray, F. Mayadas, & M. Vardi (Eds.), *Globalization and offshoring of software* (Ch. 6). New York, NY: Association for Computing Machinery.

Center for Public Integrity. (2014). Counterfeit chips plague Pentagon weapons systems. Retrieved from https://www.publicintegrity.org/2011/11/07/7323/counterfeit-chips-plague-pentagon-weapons-systems

Cooper, S. (2009). How China steals U.S. military secrets. *Popular Mechanics*. Retrieved from https://www.popularmechanics.com/military/a746/3319656/

Dean, J., & Li, L. (2002). Issues in developing security wrapper technology for COTS software products. In *Proceedings of the First International Conference on COTS-Based Software Systems*. New York, NY: Springer.

Dorofee, A., Woody, C., Alberts, C., Creel, R., & Ellison, R. (2013). *A systemic approach for assessing software supply-chain risk*. Washington, DC: U.S. Department of Homeland Security.

Du, D., & Ko, K. (2014). *Theory of computational complexity*. New York, NY: Wiley.

Grow, B., Tschang, C., Edwards, C., & Burnsed, B. (2008). Dangerous fakes: How counterfeit, defective computer components from China are getting into U.S. warplanes and ships. *Business Week*. Retrieved from https://www.bloomberg.com/news/articles/2008-10-01/dangerous-fakes

IDEF. (n.d.). IDEF family of methods: A structured approach to enterprise modeling & analysis. Retrieved from http://www.idef.com/

ISO. (n.d.). International Organization for Standardization: Standards. Retrieved from https://www.iso.org/standards.html

Johnson, R. (2011). The Navy bought fake Chinese microchips that could have disarmed U.S. missiles. *Business Insider*. Retrieved from http://www.businessinsider.com/navy-chinese-microchips-weapons-could-have-been-shut-off-2011-6

Kern, C. (2014, September). Securing the tangled web: Preventing script injection vulnerabilities through software design. *Communications of the ACM*, *57*(9), 38–47.

Ladyman, J., Lambert, J., & Wiesner, K. (2013). What is a complex system? *European Journal for Philosophy of Science, 3*, 33–67.

Lindqvist, U., & Jonsson, E. (1998). A map of security risk associated with using COTS. *IEEE Computer*, *31*(6), 60–66.

Maule, R. (2016). Complex quality of service lifecycle assessment methodology. In *Proceedings of the 5th International Conference on Big Data*. San Francisco, CA: IEEE.

Maule, R. (2017). *SEA Cyber Figure of Merit (CFOM): Tactical systems cybersecurity assessment*. Monterey, CA: Naval Postgraduate School.

Maule, R., Jensen, J., & Gallup, S. (2014). *Trident Warrior Analysis Reports 2011–2013.* Norfolk, VA: U.S. Fleet Forces Command.

Maule, R., & Lewis, W. (2011). Performance and QoS in service-based systems. In *Proceedings of the World Congress on Services Computing*. Washington, DC: IEEE.

McMullen, T. (2015). It probably works. *Communications of the ACM*, *58*(11), 50–54.

National Research Council. (2005). *Network science*. Washington, DC: National Academies Press.

Rossi, B. (2012). Security backdoor found in China-made US military chip. *Information Age*. Retrieved from https://www.information-age.com/security-backdoor-found-in-china-made-us-military-chip-2105468/

Space and Naval Warfare Systems Command (SPAWAR). (2015). *Cybersecurity figure of merit*. San Diego, CA: SPAWAR 58000.

Tiropanis, T., Hall, W., Crowcroft, J., Contractor, N., & Tassiulas, L. (2015). Network science, web science, and Internet science. *Communications of the ACM*, *58*(8), 76–82.

Cybersecurity: Converting Shock Into Action (Part 2)

Paul Shaw—Defense Acquisition University

Robert L. Tremaine—Defense Acquisition University

Abstract

Last year, the authors presented Part 1, which focused on a discussion on policy/directives and then explored the efficacy of the DoD's cybersecurity strategy and associated actions taken to date—all intended to safeguard the efficacy of DoD systems. The goal of the research in Part 2 is centered on the design and implementation of the cybersecurity training intended to achieve the key cybersecurity behaviors to meet that end. The Kirkpatrick Learning Level framework is used to help translate learning objectives into security and resilience critical behaviors for organizational oversight. The process of translating Knowledge, Skills, and Attitudes (KSAs) into learning objectives and workplace behaviors is also discussed. However, what the workforce actually applies in the workplace is the most important part of the equation, especially its correlation to expected outcomes. Part 2 addresses just that. The DoD will be hard-pressed to achieve any mission assurance objectives for security and resilience without recognizing that (1) cybersecurity critical learning behaviors require commitment at all levels—individual, team, and organizational; and (2) cybersecurity must be viewed as more of a dilemma where emerging threats will surface continuously and must be assessed with regular frequency to ensure the viability of the DoD's weapon systems' lethality.

Introduction

In March 2019, the Secretary of the Navy (SECNAV) released an extensive *Cybersecurity Readiness Review*. His uncomplimentary readiness review reinforced the findings of numerous other reports (e.g., reports by the Director National Intelligence [DNI]; Office of Management and Budget [OMB]; Government Accountability Office [GAO]; DoD Inspector General [IG]; Defense Science Board [DSB]; Director, Operational Test and Evaluation [DOT&E]; and other government agencies, think tanks, etc.) that concluded a cyberattack by an advanced cyber threat could easily inflict significant mission impact to the DoD. Simply stated, the DoD (and perhaps other federal agencies) is (are) not achieving their required mission assurance outcomes for cybersecurity and cyber resiliency. The response to the quintessential question for DoD cyber risk management (i.e., can the DoD as a collective handle a co-evolving, intelligent cyber threat?) is not good. Almost every assessment of the DoD and its supporting infrastructure has reaffirmed that it is woefully unprepared for attacks from a cyber peer. Even worse, the DoD continues to fall further behind year after year, and that might come as a shock to those who would depend on the DoD to prevent a catastrophic event by a cyber peer.

The DoD already has significant cybersecurity issues (i.e., Significant Mission Impact) and faces a learning culture with little understood obstacles, including the following:

- Cybersecurity is a complex, dynamic, and ambiguous domain and is becoming a dilemma.
- Cybersecurity Knowledge, Skills, and Attitudes (KSAs) exist (e.g., Newhouse et al., 2017) but are only sporadically translated into critical learning behaviors.
- The forgetting curve is no stranger to cybersecurity. Cybersecurity requires an ongoing commitment to a workplace learning environment for competencies to flourish.

- Formal (and tailored) training is only a learning antecedent. What the workforce actually applies (and practices) in the workplace with regular frequency is vitally important.
- Reinforcement of the critical behaviors is dependent on leadership's persistence to establish and maintain a strong learning culture.

Given its complexity, domain ambiguity, and dynamic nature, cybersecurity cannot depend on incidental learning. While a lot of good work has been done with cybersecurity core knowledge and tasks (e.g., Newhouse et al., 2017), it has yet to be translated into the critical behaviors required to fully embody cybersecurity learning gains. Newhouse et al. (2017) has numerous applicable KSAs for most cybersecurity workers, and the KSAs can be easily translated into Bloom's Taxonomy action verbs. However, using any learning application framework (e.g., Kirkpatrick or Brinkerhoff) to translate learning objectives into critical behaviors for organization oversight of security and resilience as far as their realization goes has not yet been implemented. The process of translating KSAs into learning objectives and behaviors is discussed with various representative groups. National Initiative for Cybersecurity Education (NICE) KSAs (Newhouse et al., 2017) have only connected learning objectives and behaviors described as follows:

- K0106—Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities
- K0110—Knowledge of adversarial tactics, techniques, and procedures
- K0112—Knowledge of defense-in-depth principles and network security architecture
- S003—Skill in evaluating the adequacy of security designs
- S0027—Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes
- S0054—Skill in using incident handling methodologies

What the workforce applies in the workplace is the most important aspect for cybersecurity learning. It is the reason for this research pursuit—and the more strategic challenge for the entire cybersecurity learning discipline, ahead.

Problem Statement: This research continues previous work that started with the DoD's cybersecurity strategy and policy. After conducting over 70 cybersecurity workshops with various DoD customers, cybersecurity assistance has transitioned to assisting program offices with their more chronic cybersecurity risk management challenges instead of a program's acute cybersecurity shortcomings.

Research Goals:

- Assist program offices with their commitment to harbor critical learning behaviors that support security management and security engineering that may lead to essential cybersecurity risk management practices for an evolving cyber threat.
- Demonstrate that implementing a robust, effective, and sustainable cybersecurity program requires a long-term and ongoing commitment and a transition from solving a problem to managing a dilemma.

The researchers posit that the DoD will be hard-pressed to achieve the desired mission assurance objectives for security and resilience without recognizing cybersecurity risk management, and that the achievement of security engineering critical behaviors must predominate at the individual, team, and organizational levels. Implementing a robust, effective, and sustainable cybersecurity risk management program will always be a foreboding challenge for program offices. Unlike decades ago, they now have to build systems that anticipate and survive a constant evolving cyber threat attack the minute systems are fielded, without the luxury of a crystal ball. Over a three and half year period, in executing over 70 cybersecurity workshops, DAU has refocused on how to best manage this dilemma versus how to solve a problem. The ability to understand this change means that learning KSAs need to be viewed and embodied as critical behaviors. In DAU's cybersecurity workshops, learners have the opportunity to practice these behaviors in rigorous case studies. Application of these behaviors beyond the classroom and back in their workplace is where the transformation begins, or where it can easily end before it begins. Without reinforcement, or time to practice, these vitally critical cybersecurity behaviors will likely succumb to the forgetting curve and place the systems they support at risk.

Background

Last year, the authors presented Part 1 and focused on a discussion on policy/directives and then explored the efficacy of the DoD's cybersecurity strategy and associated actions taken to date—all intended to safeguard the efficacy of DoD systems. The researchers intended to develop a cybersecurity approach customized for DoD acquisition organizations that characterized what it takes to implement a robust, effective, and sustainable cybersecurity program. This year, Part 2 focuses on the achievement of key cybersecurity behaviors to meet that end, including the following:

- Determining the effectiveness of security controls in support of risk management
- Evaluating the performance of security controls in support of organizational mission assurance objective
- Justifying security control development and implementation in support of organization mission assurance objectives
- Evaluating security controls at system interfaces and that span system of systems
- Appraising protection of information assets in context of a threat level for protected information assets

In addressing the above behaviors, it has become quite evident that cybersecurity for program offices is more of a dilemma than a problem. Program offices have a continual need to adapt their security posture over time to a co-evolving intelligent threat. Problems usually have solutions that can be applied to correct a risk that materialized (AKA the issue) at some point. When a car is broken, a diagnostic tool in the hands of a skilled technician can quickly determine the cause and the remedy required to return the car to working order. On the other hand, finding peace in the Middle East is a dilemma, and dilemmas cannot be solved anywhere near as easily. Instead, they require ongoing vigilance that balances a huge and complicated array of competing needs. Given its complexity, cybersecurity is a challenge where organizations need to continually test the outer edges of their learning envelopes with the understanding that there is no silver bullet.

To continue to guide this research pursuit, the authors used the same four questions to better isolate the learning implementation hurdles currently found in the DoD's Cybersecurity Strategy. The answers continue to be both informative and instructive:

1. **Have the DoD's actions (e.g., policy directives, tools, methods, etc.) met the stated and implied expectations for cybersecurity protection and resilience?** (Updated in Part 2)

The answer is still no. The DoD is vulnerable to crippling cyberattacks by cyber peers that could impose significant loss of life, equipment, and ability to execute mission.

DOT&E's assessment in their FY2018 annual report to Congress (Behler, 2019) can be summarized with the following comments:

> DOD missions and systems remain at risk from adversarial cyber operations. Operational tests continued to <u>discover mission-critical vulnerabilities</u> [emphasis added] in acquisition programs. (p. 229)
>
> Test and assessments in FY18 again found that low-capability attack techniques too often <u>posed a risk for disrupting operational missions</u> [emphasis added]. (p. 232)

The tone of the current DOT&E summary is very similar to previous warnings from their annual reports of FY15, FY16, and FY17 (Behler, 2018; Gilmore, 2017; Hall, 2017).

An uncomplimentary review provided in the March 2019 SECNAV *Cybersecurity Readiness Review* summarizes,

> To restate, the DON culture, processes, structure, and resources are ill-suited for this new era. The culture is characterized by a lack of understanding and appreciation of the threats, and inability to anticipate them, and a responsive checklist behavior that values compliance over outcomes, antiquated processes and governance structures that are late to respond to dynamic threats, and an enterprise whose resources are required for warfighting and defense in this environment. The net-net is that the DON is preparing to fight tomorrow's kinetic war, which may or may not come, while losing the global cyber enabled information war. (p. 7)

These results are reinforced by numerous other open source reports from the DNI, the OMB, the GAO, the DoDIG, the DSB, the DOT&E, other agency inspector generals, RAND Corporation, and numerous others—a cyberattack by an advanced cyber nation states could inflict significant mission impact to the DoD and its supporting infrastructure. This conclusion can be drawn from at least 100 different reports of cybersecurity assessments over the last eight years—a sophisticated cyberattack could inflict significant impact to DoD missions, with possibly substantial losses of life, equipment, and supporting infrastructure (Coates, 2019). Current risk mitigation strategies are not tightly connected to mission assurance imperatives in the face of a growing hostile cyber environment. In 2017, a RAND study found that "cybersecurity risk management does not adequately capture the impact to operational missions nor is it designed in" (Snyder et al., 2017, p. ix). Snyder et al. (2017) went on to say that the policies governing cybersecurity are better suited for simple, stable, and predictable environments leading to significant gaps in cybersecurity risk management. Without more critical thinking about ongoing risk management of an evolving cyber threat, future studies are likely to announce the same conclusion—the DoD is vulnerable to crippling cyberattacks by cyber peers that could impose significant loss of life, equipment, and ability to execute missions.

2. **What are the metrics and have they been effective?**

The answer is still no. Extensive DoD cyber activities are not achieving measurable outcomes of secure and resilient systems. Most DoD metrics measure activity instead of outcomes of systems of system security and resilience. While there are numerous metrics that could be cited, the authors believe the following three metrics best sum up DoD cybersecurity effectiveness: (1) comments on cyber survivability from DOT&E open source annual reports to Congress; (2) the SECNAV *Cybersecurity Readiness Review* of cybersecurity risk with who has the largest Dark Web footprint of stolen sensitive data; and, (3) the number of open cybersecurity recommendations for remediation as reported by the DoD Inspector General (IG).

DOT&E Comments From Cyber Tests on Effectiveness

DOT&E has conducted over a hundred operationally realistic cyber-threat tests over the last eight years. Only a few programs during that time achieved cybersecurity survivability objectives. In the last two DOT&E open source annual reports to Congress, successful ratings included: one instance of “demonstrated a robust cyber network defense to protect against an operationally realistic cyber threat opposing force” (Behler, 2018, p. 130), two instances of “survivable in a cyber-contested environment” (Behler, 2019, pp. 49, 53), and one instance of “secure against a cyber threat having limited to moderate capabilities” (Behler, 2019, p. 15). In this and previous DOT&E open source annual reports to Congress, the more frequent ratings are

- “not survivable in a cyber-contested environment” (Behler, 2019, p. 21),
- “vulnerabilities identified during earlier testing periods still had not been remedied” (Behler, 2019, p. 23),
- “the system remains vulnerable to cyber-attack” (Behler, 2019, p. 94),
- “has cybersecurity vulnerabilities that can be exploited” (Behler, 2019, pp. 103, 105), and/or
- “cybersecurity testing identified deficiencies” (Behler, 2019, p. 144).

Please note the above instances with page references are for different systems traceable through page references. The issue is less about cybersecurity execution by a specific program and more about an ongoing trend of DoD system effectiveness against realistic cyber threats.

DoD Protection of Sensitive Information

The lack of achieving outcomes is best demonstrated by the loss of classified and controlled unclassified information (Nakashima & Sonne, 2018). A recent *Wall Street Journal* article described the armed forces under constant cyber siege by relentless foreign actors (Lubold, & Volz, 2019). The loss of sensitive information has a significant effect on the Department of Defense (DoD) for lethality and technological superiority (Mattis, 2018). Estimates on the value of losses of intellectual property from the United States are up to $600 billion (Mattis, 2018). According to the White House, “The United States cannot afford to have sensitive government information or systems inadequately secured by contractors. Federal contractors provide important services to the United States Government and must properly secure the systems through which they provide those services” (Trump, 2018, p. 7). The DoD implemented DFARS 252.204-7012 to require contractors to protect unclassified sensitive DoD information, defined as Covered Defense Information (CDI), on their networks. SECNAV (2019) concluded that “competitors and potential adversaries have exploited DON information systems, penetrated its defenses, and stolen massive amounts of national security IP. This has lessened our capabilities and lethality, while strengthening their offensive and defensive capabilities” (p. 4). The emerging DoD vision sees a shared responsibility developing between the DoD and its contractors on the protection of sensitive information regardless of its location (DoD, 2018a, 2018b).

DFARS 252.204-7012 is now applied to all new contracts and requires contractors to protect CDI on their networks. Concerning effectiveness of these activities, the metric that the SECNAV used in his *Cybersecurity Readiness Assessment* is applicable.

> While there are many ways to measure cybersecurity risk, one indicator of vulnerability is how much data about an organization is available on the Dark Web. When compared to Fortune 500 companies, the US government has the largest collective Dark Web footprint. Of the 59 government agencies, the DON led the government with the largest Dark Web footprint. (SECNAV, 2019, p. 8)

Of particular concern should be the ability for entities to detect if they are breeched. Nine of the 129 security requirements in the National Institute of Standards and Technology (NIST) concern the ability to perform audit of unusual activity on the network. In the redacted DoJ, Office of Inspector General report, *Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process,* dated March 2019, "the FBI had 721 Special Agents dedicated to cyber investigations, including cyber victim notifications" (p. 1). Over the period from November 2014 to December 2017, "Cyber Guardian had 16,409 cyber incidents and 20,803 victim notifications" (DoJ, 2019, p. 12). Of special note was another revealing comment: "According to FBI personnel, victims of cyber intrusions are typically identified by the FBI or its partner agencies in the course of their investigative activities. As a result, many cyber victims, most of which are companies or organizations, are unaware that they are victims of an intrusion until the FBI notifies them" (DoJ, 2019, p. 1).

Open DoD Cybersecurity Recommendations for Remediation

The DoD tends to be a leader in the federal government and not to be forced to remediate open cybersecurity recommendations. A DoD Inspector General (IG) redacted report (DoDIG, 2019) states that "recently issued cybersecurity reports indicate that the DoD still faces challenges in managing cybersecurity risk to its network. Additionally, as of September 30, 2018, there were 266 open cybersecurity-related recommendations, dating as far back as 2008" (p. 6). As noted in our previous paper, "FISMA requires that each Federal agency conduct an annual independent evaluation to determine the effectiveness of the agency's information security program and practices" (DoD IG, 2019, p. 1). Prior independent assessment of DoD cybersecurity maturity, using the Cybersecurity Framework categories of identify, protect, detect, respond, and recover, tended to rank the DoD at the lowest levels of maturity of any federal agency (OMB, 2017). The DoD IG (2019) found that

> the DoD needs to continue focusing on managing cybersecurity activities in four of the five NIST Cybersecurity Framework functions—Identify, Protect, Detect, and Respond, primarily in the Framework categories of governance, asset management, information protection processes and procedures, identity management and access control, security continuous monitoring, detection processes, and communications. (p. 6)

3. Is the DoD headed in the right direction?

The answer is still partly. The DoD has shown a willingness to create policy and strategy. Senior leadership has been willing to examine itself in very critical ways. Several senior leaders have shown extraordinary vigilance by instituting major initiatives in cybersecurity reform including the Acting Secretary of Defense; the Secretary of the Navy; Director, Operational Test and Evaluation; Assistant Secretary of the Navy for Research, Development, and Acquisition; and Director, Defense Contracting Management Agency. Numerous operational commands are taking positive steps as well with self-reporting and taking corrective action.

> DOT&E performed an assessment of a major command which identified several vulnerabilities that could impact mission assurance. Senior leadership at the command self-reported to senior DoD leadership that the command's mission assurance posture was potentially degraded, and made mitigation of these vulnerabilities a top priority. [emphasis added] (Behler, 2019, p. 231)

Additionally, there have been isolated pockets of excellence within the DoD. The Army's Warfighter Information Network-Tactical (WIN-T) Increment 2 Program Office did an exceptional job of becoming a cybersecurity leader and innovator of cybersecurity acquisition and operations best practices. The Army's WIN-T Increment 2 Program Office set a high bar. The DoD's ability to assure senior leadership of mission assurance, in spite of a cyber peer threat, can be much higher once acquisition programs "demonstrate they have a robust cyber network defense to protect against an operationally realistic cyber threat opposing force" (Behler, 2018, p. 130).

A group with potential to do more for cybersecurity is the DoD Acquisition Workforce. However, SECNAV (2019) aptly noted that

> Cybersecurity is largely viewed as an IT issue and is not integrated across all operations and activities of the organization. The current approach is characterized by vertical stovepipes of responsibility which ignore the reality that information and cybersecurity require a horizontal, systems approach across all aspects of the organization's activities and operations. This horizontal approach is extremely important for without it, the DoN cannot achieve cybersecurity. (p. 7)

The DoD acquisition workforce would be well-served if it approached cybersecurity as a dilemma instead of a problem. To make matters worse, many in the acquisition community have either deflected or not fully embraced their role in cybersecurity and the need to adapt to the persistent threat. It's vitally important to elevate the acquisition community's knowledge of cybersecurity risk management through better implementation of systems security engineering, the ability to adapt to advancing threats, and integration with cyber operations. The acquisition workforce needs to transition from a "compliance construct" for cybersecurity to one of cybersecurity for operational "mission assurance." More systems might achieve in operational test adversarial assessments and fulfill operational commanders' mission assurance needs if there was a transition of approach, culture, and workforce attitudes.

The cyber threat is evolving and changing as Snyder et al. (2017) indicated:

> Capabilities of potential adversaries are growing, and the changing technologies introduce new vulnerabilities over time. This evolution means that static solutions for cybersecurity management are unlikely to be effective; cybersecurity solutions need to be adaptive. Creating defensive barriers in the form of security overlays that respond to discovered vulnerabilities is by nature insufficient to protect against future, unknown threat vectors [emphasis added]. (p. 7)

Actors with the ability to exploit the DoD's systems are growing at a staggering rate:

> Recent advances in cyber technologies indicate that automation—and even artificial intelligence—are beginning to make profound changes to the cyber domain. Warfighters and network defenders must prepare for the onslaught of multi-pronged cyberattacks [emphasis added] across both

> critical mission systems and the multitude of supporting systems and networks that enable these missions. (Behler, 2019, p. 229)

To keep pace with the threat, the DoD acquisition workforce needs to step up their game.

4. What industry best practices should the DoD adopt and why?

There are numerous. Industry best practices have concentrated their efforts on resilience, trustworthiness and continual testing. Intel, Google, Microsoft, Netflix, major financial institutions, and other cybersecurity leaders have taken an enterprise approach to cybersecurity. Their approaches include active engagement of cybersecurity by senior leadership and robust workforce cybersecurity involvement. As stated by SECNAV (2019),

> The enterprise approach is not just about the systems and management; it also includes robust involvement by the workforce. Many companies simply fire personnel, from the C-Suite to the line level, who fail to follow established cybersecurity policy and processes. They also have very active CEO and CIO/CISO-led Cybersecurity committees and working groups that meet on a regular basis which include business unit, technology, risk management, and executive leadership. (p. 34)

Best in class cybersecurity companies have transitioned their security posture traditional security activities to emerging security concepts. Their best practices include rapid adoption of transformational emerging security technologies (such as for access management); extensive monitoring of network and system health, especially for configuration management and access management; and extensive and continual testing (extensive developmental testing, internal adversarial testing, bug bounties, etc.).

An example of an industry best practice is the “zero-trust model.” This model was a core element of the Army’s WIN-T Increment 2 security posture. SECNAV (2019) described the zero-trust architecture as follows:

> With a Zero-Trust model, successful companies have addressed both careless behaviors and malicious intent by granting trust only to those who have securely proven their identity. Having done so, their subsequent access to resources is limited to the least amount of access required. Successful Zero-Trust designs include processes that ensure all resources are accessed securely, adopt a least-privileged strategy strictly enforcing access control, and continuously monitor the enterprise ecosystem. Everyone and everything is constantly validated, with zero exemptions. (p. 36)

The more mature cybersecurity companies have a wider focus than just system protection to that of dynamic performance evaluation. The September 2016 DoD Defense Science Board report on cyber defense management recommended

> examining the attack data to determine what is working well, what is not, where changes need to be made, and where investment is required to better defend against troublesome or emerging threats to move beyond a compliance approach towards a more dynamic performance evaluation. (p. 11)

These companies have adopted a security posture of adaptability and innovative thinking in response to impending cyber threats.

Will this type of thinking eventually become pervasive in the DoD? There are isolated pockets of excellence in the DoD exhibiting the required change of approach, culture, and workforce attitudes to execute these best practices. Such a transition just needs to occur across a much wider swath of the acquisition workforce and their DoD contractors in order to respond to impending cyber threats.

Assumptions

As with any research study, assumptions generally help characterize the research constraints as well as the prevailing environmental domain. While strikingly provocative, the following (and persistent) assumptions reinforce today's cybersecurity operating envelope:

- Cybersecurity is a decaying function—static cybersecurity assures a declining security posture.
- No system is without malware—every system has an inherent vulnerability just waiting to be exploited.
- Organizations rely too much on technology for security and don't sufficiently consider the people and process components.
- The seemingly most secure system often fails to acknowledge that it can be affected by a higher level threat (i.e., any system can be misconfigured).
- Cybersecurity policy stands at the outcome level; acquisition guidance and implementation below the outcome level is subjective (i.e., outcome level is typically characterized as "design for the fight")
- Most programs undershoot "adequate security"—many operate under a false sense of security until they discover they did not sufficiently manage realistic and likely operational risks.
- The DoD may not be proactive enough to exploit its own systems to withstand advanced threats.
- Politics can trump engineering. Systems security engineering is constrained in pursuing a preferred solution set due to required integration with legacy components and systems, lack of control over interfacing systems, and a preference for functionality over security.
- If user behavior is monitored and proper user behaviors can be enforced, the chance to reduce a significant attack surface is increased. Significant benefits for good user disciple: cost of implementing an effective security posture is reduced, and probability of successful detection and recovery increased. Money is a poor substitute for discipline (especially enforced user security behaviors).

Research Methodology

The researchers treated the cybersecurity skills captured in the NICE KSAs as the basis of the required critical learning behaviors. The researchers wondered what if they were treated as static, and not part of continuous process of learning and reinforcement (e.g., Monitor, Encourage, Reinforce, and Reward [MERR]). What if the acquisition workforce did not learn or retain the critical behaviors? These questions set the stage for what could be seen as more deterministic outcomes since

- Without a strong bridge in the form of metrics between what students learned in class (Level II) and what they applied in the workplace (Level III), it is more difficult to connect the two, and
- Without the evidence, organizations would be hard-pressed to confirm the resources they allocated to Level II learning gains actual paid off in the workplace.

The directorate’s intact teams who attended the workshop also previously committed to connecting Level II learning objectives with the Level III critical behaviors. Just as importantly, their leadership committed to what Kirkpatrick calls its required drivers (i.e., MERR) to assure their Level III achievements (Kirkpatrick & Kirkpatrick, 2016, p. 56). Without them, a key feedback mechanism would be missing, and accountability opportunities would be lost. However, the more important aspect surrounds the abilities and attitudes of the learners to apply what they learned in the workshop back on-the-job (i.e., Level III that doesn’t atrophy), and what results their learning afforded. Furthermore, what will happen and what needs to happen to strengthen the bridge between Learning Level II and Learning Level III? The achievement of these Learning Level III critical behaviors represents the litmus test. Through a suitable dose of feedback (i.e., MERR), Learning Level III critical behaviors and Level IV results are more achievable later.

The Forgetting Curve

Closely tied to any learning is the unforgettable “forgetting curve,” originated by Herman Ebbinhaus (Murre, 2015). He characterized it in a simple formula:

R = e^(-t/s), where R = Recall; e = Euler’s constant (2.71); t = time passed; and s = strength of memory.

He proved that about 80% of what we learn we forget in 30 days if there is no reinforcement (i.e., “forgetting curve”), and it still holds true today. Why is that important for cybersecurity? Aside from remembering and applying the nine framing assumptions originally described in this study, and in the context of an ever-evolving functional discipline that is more a dilemma than a problem, dismissing it would be a dangerous proposition. MERR is no antidote, but it certainly keeps the affected individuals’ consciousness on high alert, and rightfully so.

Cybersecurity Workshop Structure

To build greater cybersecurity knowledge and raise awareness for acquisition professionals, DAU conducted various workshops for diverse audiences. Figure 1 depicts the focus of these workshops and the variability between technical execution and technical oversight.

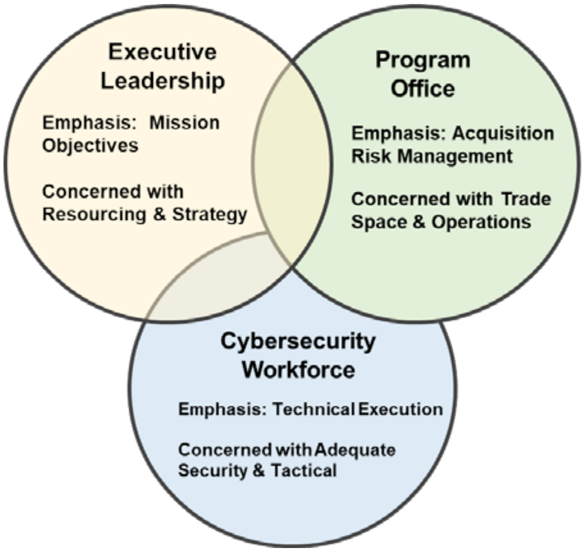

Executive Leadership
Emphasis: Mission Objectives
Concerned with Resourcing & Strategy
Program Office
Emphasis: Acquisition Risk Management
Concerned with Trade Space & Operations
Cybersecurity Workforce
Emphasis: Technical Execution
Concerned with Adequate Security & Tactical

Figure 1. **Customer Composition in Workshops**

The critical questions for these workshops have been: Will DAU's cybersecurity workshop enable the individual to develop a competence (either a tactic, technique, protocol, or procedure) or behavior that will enable an organizational outcome? Will the organization make a commitment in monitoring, encouraging, reinforcing, and rewarding to achieve learning gains in the workplace? Possibly the most successful of our cybersecurity workshops has been a series of three workshops over multiple days. Figure 2 covers the essence of the three workshops—NIST Systems Security Engineering, Threat-Based Engineering, and Active Cyber Defense. These workshops were designed to help the participants understand security principles, cyber threat and their tactics, and integration of acquisition with cyber operations. The compilation of these workshops addresses the horizontal issues brought up by SECNAV (2019)*.* The SECNAV (2019) well understood that cybersecurity requires "a horizontal, systems approach across all aspects of the organization's activities and operations" (p. 7).

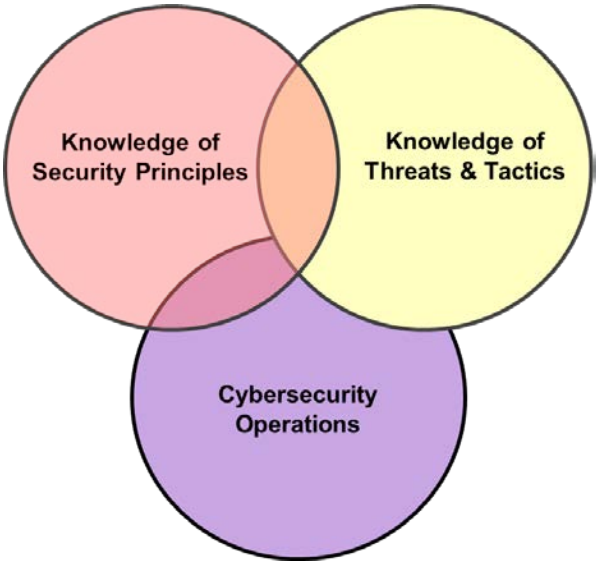

Knowledge of Security Principles
Knowledge of Threats & Tactics
Cybersecurity Operations

Figure 2. **Types of Cybersecurity Workshops**

The NIST Systems Security Engineering (SSE) uses the NIST 800-160 (Vol. 1 & 2) to cover the standards and constructs of system trustworthiness and system resilience. The NIST SSE workshop was designed to give the participants time to apply best practices outlined in NIST publications 800-160 (Vol. 1 & 2; Ross, McEvilley, & Oren, 2017; Ross et al., 2018). Three core behaviors are taught and practiced in the NIST SSE workshop:

- Construct a comprehensive and holistic system view while addressing stakeholder security and risk concerns;
- Apply input to analyses of alternatives and to requirements, engineering, and risk trade-off analyses to achieve a cost-effective security architectural design for protections that enable mission/business success; and
- Evaluate the effectiveness and suitability of the security elements of the system as an enabler to mission/business success.

NIST has done an exceptional job of understanding standards and techniques and developing a core process in each of the various volumes. For example, Ross et al. (2017) state,

> The ultimate objective is to address security issues from a stakeholder requirements and protection needs perspective and to use established engineering processes to ensure that such requirements and needs are addressed with the appropriate fidelity and rigor across the entire life cycle of the system. (p. viii)

For system security engineering trustworthiness, our desired outcome is to develop and demonstrate the evidence necessary to support assurance claims and to substantiate the determination that the system is sufficiently trustworthy. Ross et al. (2018) note that “the ultimate objective is to obtain trustworthy secure systems that are fully capable of supporting critical missions and business operations while protecting stakeholder assets, and to do so with a level of assurance that is consistent with the risk tolerance of those stakeholders” (p. ix). For system security resiliency, the desired outcome is focused on designing security risk management activities, producing related security risk management information, and advising the engineering team and key stakeholders on the security-relevant impact of threats and vulnerabilities to the mission/business supported by the system.

This is the pre-course email sent to the workshop participants:

> You will do a capstone case study as part of a team for either system trustworthiness or system resiliency. While we have case studies for you to work on—if you should desire to nominate a project that you are working on as either a trustworthiness or resiliency exercise—we will accommodate it. The only caveat is that the training is being executed in Unclassified spaces. We have done other DoD systems as exercises (either trustworthiness or resiliency) in previous SSE workshop sessions in unclassified spaces. Please talk to me on day 1 with your proposal. I suspect there is a high probability that we can figure out how to make it work.

The participants nominate a problem they have in their environment. The goal is to help participants understand how to implement the standards and techniques to achieve an outcome through a series of exercises and case studies. The capstone exercise validates whether their system is trustworthy and resilient.

In the NIST SSE workshops, participants raised the following issues that they felt have limited their ability to execute a particular security standard and/or resilience technique:

- Can I change the design/architecture?
- Can I change configuration?
- Ability to manage interfaces?
- Can I contain/isolate/segment trust relations?
- Can I implement new processes?
- Can I automate a process?
- How will I monitor & enforce user behavior?
- Can I trade off/restrict functionality?
- What capability will a newer technology provide (will my users be able to implement the technology)?

The fact that these types of questions are occurring in the workshop case studies is very encouraging. The next step is to follow up with the workshop participants to ensure the behaviors of construct, apply, and evaluate are underway at their workplaces. There’s no guarantee that the learners will have enough opportunities to apply everything they learned in the workshop. What needs to happen in the workplace to combat the likely consequences of forgetting curve? Without a coach or mentor, how do they get to the point where they sustain the cognitive connection to the original learning behavior—and how do we measure it? The workplace has to establish surrogate scenarios that refresh and reinforce the critical learning behaviors—and what tools are the most appropriate.

Results and Findings

Individuals enter the workshops with a wide variance of cybersecurity experience and knowledge levels—novice to experienced practitioner. There seems to be several revelations that occur during a workshop that would likely increase the chance that a student will apply appropriate risk management and security engineering constructs and behaviors to their situation after the conclusion of a workshop. Students progress through the following stages: understanding cybersecurity is a severe security threat; acknowledging the cyber threat is not static, but evolving; accepting that their system/program needs to do something about evolving cyber threats; adapting their cybersecurity security posture if the cyber threat changes; committing to cybersecurity risk management as a continual, ongoing effort; and becoming an effective agent of change to achieve meaningful outcomes. Depending on the maturity of the student and their organization, individual progression can stop at any point in the cycle of progression. During these workshops, the following common themes surface:

- Workshop participants usually start the workshops looking for prescriptive answers. They hope to find a fix to their cybersecurity problem.
- The initial focus is frequently satisfying some external entity. The most common DoD focus is to satisfy an Authorizing Official (AO). More advanced programs will set a goal of succeeding against a capable adversarial assessment sponsored by a DoD Operational Test Agency (OTA). While both are worthy objectives, their real focus should be one of mission assurance.
- Often, they are not creating a solution set that can adapt if the threat should change. Most want to stop after finding a single possible solution, instead of creating a solution set.
- They want to make the threat static and then optimize to a static threat. Accepting an evolving threat is a significant strain on people and resources.
- They need to achieve a construct of self-assessment and continual testing—such that achievement of either an ATO/ATC or passing an OTA assessment—are just part of an ongoing process for cyber risk management to achieve mission assurance.

The core question simply stated became “What initial successes will likely occur as you consistently apply what you learned?” In the researchers’ Part 1 of this study, we examined the Western Naval Audit Service in learning and applying critical cybersecurity behaviors from our workshops. This particular group was highly motivated and had committed leadership. Kirkpatrick calls it having required drivers (i.e., monitor, encourage, reinforce, and rewards) to assure their Level III achievements (Kirkpatrick & Kirkpatrick, 2016, p. 56). Since their initial series of cybersecurity workshops, this group offered to the SECNAV’s office to bid for a cybersecurity audit. The SECNAV assigned Western Naval Audit Service a critical audit issue concerning fleet cybersecurity readiness. This audit is underway and should be back to the SECNAV’s office for review before the end of 2019. To go from no cybersecurity audit experience to conducting a major fleet readiness cybersecurity audit review was a major commitment by this group and the start of objective measurable outcomes in the form of secure and resilient systems.

Across multiple workshops, we have seen statistically significant changes in attitudes towards the behaviors. The following qualitative comments across various workshops summarize the trend seen across the workshops.

- Participant 1—Right now, as a novice, I would say my biggest challenges are ensuring I have a full and complete understanding of all the components, and having a clear vision of putting all this into play …
- Participant 2—The biggest challenge is simply a matter of scope vs. resources. We all face this of course, so finding time to keep momentum requires focus that is sometimes difficult.
- Participant 3—I was impressed that the training was compressed into two days. So much material was covered! … I think that improvement will come from continuing the activity so it is not a one and done …
- Participant 4—This workshop helped me better understand the requirements and how to convey that importance to our customers …
- Participant 5—When looking at the security posture of an asset, I will now ask the questions to determine what the priority result is for this asset and then look at the systems needed to attain that goal/result. …
- Participant 6—I'm standing up a lab for a new C2P effort. … It is aimed at replacing the legacy C2P over the next decade. I expect to apply the techniques learned in this workshop during our IPTs …
- Participant 7—This course has made me more important as a resource to others around me. … Already, leaving the class, was able to connect to a resource in the Cloud Broker to the O(ffice)365 Broker …

From the above comments, the described student progression can be seen. These participants are starting to understand cybersecurity is a severe security threat, acknowledging the cyber threat is evolving, accepting their responsibility to do something, adapting their cybersecurity security posture, and committing to ongoing cybersecurity risk management. If these participants receive reinforcement from their organization, there is a significant probability for meaningful outcomes to occur. If we can start to have more of the acquisition workforce to exhibit the same types of attitudes – our operational forces might have a chance against when facing a cyber peer.

Conclusion

The number of cyber threat actors who have the ability to exploit the DoD's systems is growing at a staggering rate while too many people involved in the acquisition community may not have fully embraced (or even understand) their role in cybersecurity. It's vitally important to elevate the acquisition community's knowledge of all cybersecurity risks in order to more carefully plan, decide, and act for inescapable and impending cybersecurity threats. Admittedly, the danger signs are very telling, and they're not good.

In Part 2 of this research project, the authors reinforced how behaviors learned in workshops could be instituted in a participant's work environment. The researchers posit that the DoD will be hard-pressed to achieve the desired mission assurance objectives for security and resilience without recognizing that (1) cybersecurity risk management and security engineering critical learning behaviors require commitment at all levels—individual, team, and organizational; and (2) cybersecurity is a domain that must be viewed as a dilemma where there is no one-size-fits-all solution, nor can it be treated as a static problem. Cybersecurity threats will never wane in frequency or severity. Its asymmetric nature is too great. Without constant vigilance, the United States will lose the cybersecurity war.

Thankfully, the commitment from numerous senior DoD leaders is growing. Outside the DoD, there has been a willingness from numerous organizational leaders (e.g., the intelligence community, DOT&E, IG, audit service, chartered boards, think tanks, etc.) to take similar action. And programs like the WIN-T Increment 2 Program Office have demonstrated what it takes to achieve cybersecurity excellence at a given juncture. If the remaining acquisition workforce steps up to the cybersecurity learning challenge, the negative trends discussed at the beginning of the paper might just start to reverse course, resulting in a much more favorable heading.

References

Behler, R. (2018). *Director, Operational Test and Evaluation FY 2017 annual report.* Washington, DC: DoD*.* Retrieved from https://www.dote.osd.mil/pub/reports/FY2017/

Behler, R. (2019). *Director, Operational Test and Evaluation FY 2018 annual report.* Washington, DC: DoD*.* Retrieved from https://www.dote.osd.mil/pub/reports/FY2018/

Coates, D. (2019). *Worldwide threat assessment of the U.S. intelligence community*. Retrieved from Director, National Intelligence website: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Defense Federal Acquisition Regulation Supplement (DFARS), 48 C.F.R. 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (2016).

DoD. (2018a). *Fact sheet: 2018 DoD cyber strategy and cyber posture review.* Retrieved from https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL.pdf

DoD. (2018b). *Summary: Department of Defense cyber strategy 2018*. Washington, DC: Author. Retrieved from https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

DoD Chief Information Office. (2014). *Cybersecurity* [DoDI 8500.01]. Washington, DC: Author. Retrieved from http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

DoD Defense Science Board. (2016). *Cyber defense management.* Retrieved from https://www.acq.osd.mil/dsb/reports/2010s/Cyber_Defense_Management.pdf

DoD Inspector General. (2019). *Summary of reports issued regarding Department of Defense cybersecurity from July 1, 2017, through June 30, 2018.* Retrieved from https://media.defense.gov/2019/Jan/11/2002078551/-1/-1/1/DODIG-2019-044.PDF

DoJ. (2019). *Audit of the Federal Bureau of Investigation's cyber victim notification process.* Retrieved from https://oig.justice.gov/reports/2019/a1923.pdf

Geurtz, J. (2018). *Implementation of enhanced security controls on select defense industrial base partner networks.* Washington, DC: Assistant Secretary of the Navy for Research, Development, and Acquisition.

Gilmore, J. (2017). *Director, Operational Test and Evaluation FY 2016 annual report.* Washington, DC: DoD*.* Retrieved from http://www.dote.osd.mil/pub/reports/FY2016

Hall, J. (2017). *Developmental Test and Evaluation FY 2016 annual report.* Washington, DC: DoD. Retrieved from https://www.acq.osd.mil/dte-trmc/docs/FY2016_DTE_AnnualReport.pdf

Kirkpatrick, J., & Kirkpatrick, W. (2016). *Four levels of training and evaluation*. Alexandria, VA: ATD Press.

Lubold, G., & Volz, D. (2019). Navy 'under cyber siege' by Chinese hackers. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/navy-industry-partners-are-under-cyber-siege-review-asserts-11552415553

Mattis, J. (2018). *Establishment of the Protecting Critical Technology Task Force* [Memorandum]. Washington, DC: Secretary of Defense.

Murre, J. M. J., & Dros, J. (2015). Replication and analysis of Ebbinghaus' Forgetting Curve. *PLoS One, 10*(7). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4492928/

Nakashima, E., & Sonne, P. (2018). China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?noredirect=on&utm_term=.8836302b51d5

Newhouse, W., Keith, S., Schribner, B., & Witte, G. (2017). *National initiative for cybersecurity education (NICE) cybersecurity workforce framework* [NIST Special Publication 800-181]. Retrieved from National Institute for Standards and Technology website: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Office of Management and Budget (OMB). (2017). *Federal Information Security Modernization Act of 2014: Annual report to Congress.* Washington, DC: Author. Retrieved from https://www.hhs.gov/sites/default/files/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD[AT&L]). (2015). *Operation of the defense acquisition system (Incorporating change 3, August 10, 2017).* Retrieved from http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002_dodi_2015.pdf

Ross, R., Graubart, R., Bodeau, D., & McQuaid, R. (2018). *Systems security engineering: Cyber resiliency considerations for the engineering of trustworthy secure systems* [Draft, NIST Special Publication 800-160 Volume 2]. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf

Ross, R., McEvilley, M., & Oren, J. (2017). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems* [NIST Special Publication 800-160, Vol. 1]. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

Secretary of the Navy (SECNAV). (2019). *Cybersecurity readiness review.* Retrieved from https://www.navy.mil/strategic/CyberSecurityReview.pdf

Snyder, D., Power, J., Bodine-Baron, E., Fox, B., Kendrick, L., & Powell, M. (2017). *Improving the cybersecurity of the U.S. Air Force military systems throughout their life cycles.* Retrieved from https://www.rand.org/pubs/research_reports/RR1007.html

Trump, D. J. (2018). *National cyber strategy of the United States of America*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Panel 6. International Defense Acquisition: China and Innovation

Wednesday, May 9, 2019	
12:45 p.m. – 2:00 p.m.	**Chair: Dr. Christopher P. Twomey,** Associate Professor, National Security Affairs, Naval Postgraduate School ***China's Efforts in Civil-Military Integration, Its Impact on the Development of China's Acquisition System, and Implications for the United States*** Tai Ming Cheung and Eric Hagt, University of California San Diego ***Civil-Military Fusion: Comparative Analysis of Chinese and U.S. Approaches to Defense R&D*** Nathan Picarsic and Emily de La Bruyere, Long Term Strategy Group ***Department of Defense Emerging Technology Strategy: A Venture Capital Perspective*** James Cross, Franklin Templeton, and Bill Greenwalt, The Atlantic Council

Dr. Christopher P. Twomey—Dr. Twomey is a tenured Associate Professor of National Security Affairs at the U.S. Naval Postgraduate School in Monterey, Calif. In 2004, he received his Ph.D from MIT in Political Science and joined the NPS faculty, later serving as Associate Chair for Research and as Director of the Center for Contemporary Conflict from 2007-09. Today, he works closely with the Office of the Secretary of Defense (Policy) and the State Department on a range of diplomatic engagements across Asia and regularly advises PACOM, STRATCOM, and the Office of Net Assessment.

He has been the lead organizer of the US-China Strategic Dialogue, a track 1.5 diplomatic meeting on strategic nuclear issues, since its inception in 2005. He is currently a member of the Institute of International Strategic Studies, a member of the Adjunct Staff at RAND, and has consulted for the National Bureau of Asia Research (NBR) continually since 2009.

His book—The Military Lens: Doctrinal Differences and Deterrence Failure in Sino-American Relations (Cornell, 2010)—explains how differing military doctrines complicate diplomatic signaling, interpretations of those signals, and assessments of the balance of power. Its empirical work centers on contemporary and historic Sino-American cases. He edited Perspectives on Sino-American Strategic Nuclear Issues (2008), and his work has appeared in journals such as Security Studies, Journal of Contemporary China, Asian Survey, The Washington Quarterly, Nonproliferation Review, Contemporary Security Policy, Asia Policy, Current History, and Arms Control Today, in addition to a dozen edited volumes.

He has previously taught or researched at Harvard, Boston College, RAND, the Chinese Academy of Social Sciences, and IGCC. He has lived in China several times, speaks and reads Chinese, and regularly travels to Asia.

China's Efforts in Civil-Military Integration, Its Impact on the Development of China's Acquisition System, and Implications for the United States

Tai Ming Cheung—School of Global Policy and Strategy, University of California, San Diego

Eric Hagt—School of Advanced International Studies, Johns Hopkins University

Abstract

China, under the leadership of Xi Jinping, is significantly stepping up its efforts to pursue civil-military integration—or what he calls military-civil fusion (MCF)—as an integral component of its grand development strategy of building a technologically advanced and militarily powerful state within the next one to two decades. This paper examines the making, nature, and implementation of Xi's grand MCF undertaking. This paper offers an analytical framework that seeks to provide a coherent and holistic view of the many moving parts and disparate elements of MCF through an innovation systems perspective. This framework identifies seven categories of factors that are important in shaping the structure and process of the MCF system: catalytic, input, institutional, organizational, networks, contextual, and output factors. Key dynamics that are examined in detail in the paper include the high-level leadership engagement, the influence of the external threat and technology environments, the application of new financial mechanisms such as hybrid state-private sector investment funds, the role of key state and military agencies, and the evolution of the Chinese defense acquisition system to embrace MCF.

Introduction

The defense and civilian economies in China co-exist side-by-side, but their relationship has been far from harmonious or close. They are separated by deep-seated structural, normative, and operational dynamics that have limited their mutual interactions and linkages. This division was originally by design as the Communist state's founding fathers wanted to maintain tight secrecy over defense activities and prioritize the forging of the defense industrial base over civilian economic development during the height of the Cold War between the 1950s and 1970s. This rigid civil-military compartmentalization became so deeply entrenched that succeeding regimes in the post-Mao reform era have struggled mightily to bridge this yawning gap—with mixed results.

From Deng Xiaoping in the 1980s to Xi Jinping today, Chinese leaders have pursued an assortment of strategies to straddle the civil-military divide for different reasons. Deng sought to divert large segments of the defense industrial base from military to civilian production to support broader economic development. Jiang Zemin and Hu Jintao pursued an incremental approach of reducing barriers between the civilian and defense economies to promote an expanding overlap of economic activities, such as allowing civilian firms to compete for military orders and permitting defense firms to tap into the capital markets.

Xi Jinping has made civil-military integration (*Junmin Yitihua*), or what he calls military-civil fusion (MCF -*Junmin Ronghe*), a key element of his grand development strategy of establishing a technologically advanced and militarily powerful Chinese state. He has replaced the gradualist approach of his immediate predecessors in favor of a far more ambitious, high-powered, and expansive strategy that aims to establish a tightly integrated dual-use economy during his reign in power. To ensure that his goals and vision are carried out, Xi put himself in direct charge of this fusion initiative.

To address the title question of whether Xi can build a truly effective and integrated civil-military economy, this paper examines the making, nature, and implementation of his grand MCF effort. This paper offers an analytical framework that seeks to provide a coherent and holistic view of the many moving parts and disparate elements of MCF through an innovation systems perspective. This framework identifies seven categories of factors that are important in shaping the structure and process of the MCF system. These factors will be examined in detail in the rest of the paper. This paper begins though by providing a brief overview of the development of MCF policy in China since the beginning of the 21st century through to its embrace by Xi Jinping during the first term of his rule in the mid-2010s.

Defining Chinese Approaches to MCF

The study of MCF in China is greatly complicated by the lack of clear definition. The integration of the military and civilian economies in its broadest definition is an effort to remove the longstanding institutional and regulatory barriers between the two systems and fuse them into a single entity able to produce for both civilian and military needs. In reality, however, the two separate spheres interact in highly disparate ways depending on the local political economy conditions in which they are embedded.

The way MCF is discussed in China can be summarized by grading its related activity on a scale of integration, a MCF value chain if you will, which reflects both the efficiency and innovation gains in the system through collaboration. At the bottom is a complete division between the defense and civilian economies, a condition that has no integration in the system, is inefficient and produces little collaborative innovation. Although simplified, this was largely the state of affairs in China during the 1960s and 1970s.

The next level is defense conversion (*junzhuanmin*), which dominated civil-military interaction from the beginning of the reform era (1978) to the late 1990s. With some exceptions, this period was marked by a diversion of excess capacity in the defense industrial base, precipitated by decreased defense budgets while maintaining the sector's productive force. Integration with the civilian sector was low as this was in the main a one-way conversion process. While it helped spare the defense industrial base, efficiency and technological collaboration were low as the sector competed with the civilian sector in low-tech, consumable goods.

Since the defense industry reforms of the late 1990s, a number of additional forms of MCF have come to characterize the Chinese economy, including spin off (or military to civilian transfer, *junzhuanmin*) and spin on (civilian to military transfer, *minzhuanjun*). *Spin off* is the commercial application of a product or technology originally conceived for military purposes, while *spin on* is the reverse: technologies developed entirely within the commercial sector and adapted for defense. Both are common in the Chinese economy, which can lead to efficiency gains (particularly with relevant commercial-off-the-shelf [COTS] products). However, while some interaction is inherent in such spillover economic activity, collaboration greatly varies and is often minimal in the Chinese system.

Dual-use activity (*junmin liangyong*), on the other hand, particularly the Chinese context, implies a closer relationship between the defense and civilian sectors. While some degree of dual-use potential is intrinsic to many technologies, this refers to science and technology (S&T) programs that intentionally serve both defense and non-defense outcomes. This type of program began in earnest with China's 863 Program in the late 1980s, but has since been a central component of many national innovation projects (Cheung et al., 2016). While the level of civil-military cooperation required for such programs is substantial, these dual-use programs are frequently focused on particular technologies and limited in their effect in breaking the barriers of separation between defense and civilian participants within these programs, much less the broader economy.

The next level that has become a leading mantra of defense innovation scholars is the so-called *mincanjun*, or the participation of civilian or commercial entities in defense projects. As this domain increases its investment in research and development (R&D) and its capacity to lead the defense industry in many emerging technologies, the military is looking to encourage their participation in defense projects. *Mincanjun* clearly has the potential to produce a higher form of civil-military interaction and incorporate a much larger swath of economic and technological activity for defense purposes.

And under a final phase, there is a complete fusing of defense and civilian productive forces (*yitihua, or junmin ronghe*), where there are not two separate sectors, but a single industrial and technological ecology able to produce for both military and the national economy as needed. Such full integration would enable China to achieve maximum efficiency and technological innovation gains. While this unified system is more of a long-term aspiration than an immediate goal, Xi Jinping has emphasized that a fully integrated or fused "national strategic system" is his primary policy focus (Jingjing, 2016, pp. 19–20).

Overview of Chinese Efforts to Pursue MCF in the 21st Century

MCF has been promoted in China since the early 2000s but with little tangible success because of limited leadership engagement, unclear strategy, ineffective implementation, and weak civil-military coordination. Despite the weak progress, Chinese civilian and military authorities have viewed MCF as essential in the drive for original innovation and defense modernization.

Hu Jintao attempted to broaden MCF's scope and pushed for deeper implementation during his tenure from 2002 to 2012, although with limited success. Ultimately, Hu's aim to implement "overall coordination" stalled due to persistent obstacles such as poor coordination among top level decision-making bodies, insufficient regulatory structures to allow transfer of technology between civilian and military entities, poor intellectual property rights (IPR) protection, especially for defense industry-originated IPR, and lack of universal industry and technology standards across civilian and military sectors. While Hu's attempt at top-down leadership support should have been enough to catalyze MCF implementation, it proved insufficient to mobilize all the needed actors and agencies.

Two modest successes of Hu's push were (1) broadening the thinking on MCF away from its former limited understanding of "combining the military and civilian sectors" [*Junmin Jiehe*] to an understanding more reflective of the deep implementation required through "integration" or "fusion" of civilian and defense sectors; and (2) broadening the scope of MCF to include all available economic resources in the promotion of the defense industry, including capital, technology, human capital, facilities, and information (Alderman, Crawford, Lafferty, & Shraberg, 2014).

When Xi became China's supreme leader at the 18th Party Congress in November 2012, MCF was included in major leadership speeches and policy documents to show that the incoming regime would continue to pay attention to this issue. There was though little indication of a new direction in MCF policy. The 18th Communist Party Congress work report issued in November 2012 detailing Xi Jinping's policy agenda for his first term pointed out that the country would

> continue to follow a Chinese-style path that integrates the development of the military and civilian sectors, combine efforts to make the country prosperous and the armed forces strong, and strengthen strategic

> planning, system building as well as related laws and regulations to boost the development of military and civilian sectors in an integrated way. (Jintao, 2012)

A year later at the Third Plenum of the 18th Party Congress in November 2013 that laid out an ambitious roadmap of economic reforms, Xi and his lieutenants offered intriguing but vague hints that they were looking to inject new thinking and initiatives on MCF as part of the broader goal of undertaking comprehensive reforms of the economy and military establishment. The Third Plenum decision noted the importance of

> promoting the extensive development of military civilian fusion. Establish mechanisms for unified leadership, coordination between the military and localities, linking needs and demands and resource sharing at the national level so as to promote the joint development of the army and the people … and guiding superior private enterprises to enter into areas of military material research, development, production and maintenance. ("Decision of the CPC Central Committee," 2013)

What stood out were the references to the promotion of "extensive" MCF development, creating "mechanisms for unified leadership," and "guiding superior private enterprises" into military activities.

Xi's commitment to MCF became evident by 2015, when it was designated as a national priority and was consciously incorporated into the innovation driven development strategy (IDDS), the country's new national development strategy, which aimed to develop a strategic system and capabilities that will allow China to "implement key science and technology projects and race to occupy the strategic high ground for science and technology innovation" ("Xi Calls for Deepened Military, 2018). Key elements of this national strategic system are detailed in some of the MCF implementation plans that have been formulated since the adoption of the MCF development strategy. This includes the 13th 5-Year Special Plan for Science and Technology MCF Development issued jointly in 2017 by the Central Military Commission Science and Technology Commission (CSTC) and the Ministry of Science and Technology (MoST) that detailed the establishment of an integrated system to conduct basic cutting-edge R&D in artificial intelligence, bio-technology, advanced electronics, quantum, advanced energy, advanced manufacturing, future networks, and new materials "to capture commanding heights of international competition" (CMC Science and Technology Commission and Ministry of Science and Technology, 2017). This plan also noted the pursuit of MCF special projects in areas such as remote sensing, marine-related technology, advanced manufacturing, biology, and transportation.

Analytical Framework: The MCF Innovation System

As a starting point, it is crucial to understand that MCF is arguably one of the most ambitious industrial policy programs China has ever embarked on. MCF not only incorporates numerous traditional industry sectors (from shipping to aviation), but the industry chain of each sector including upstream R&D to downstream manufacturing. In so doing, it requires the coordination of an enormous range of bureaucratic stakeholders governing the economy. Additionally, there is the divide between the private and state-owned firms in the economy that must be managed in order for MCF to be effective. As much of China's economy is operated at the local level, a center-local dynamic also plays an important role given the national level goals and actors that MCF embodies. This decentralized system accentuates the diversity of China's economy geographically, a phenomenon that profoundly impacts a coherent national MCF strategy. If all of this was not sufficiently challenging, underlying all of the above is the separation between the military and civilian systems within China that first and foremost must be tackled in order for MCF to be conceivable.

One analytical approach to address this complexity and confusion is to view MCF as a hybrid eco-system comprised of institutional arrangements, organizations, networks, inputs, outputs, and various other factors. This paper applies the notion of an innovation system derived from the systems of innovation and public policy process literature to examine the Chinese approach to MCF. Innovation systems are complex, constantly evolving eco-systems that include "all important economic, social, political, organizational, institutional and other factors that influence the development, diffusion and use of innovations" (Edquist & Johnson, 2005). Innovation is of central importance to MCF because its mantra is about finding new or improved ways of meeting defense and dual-use needs faster, better, and cheaper.

A diverse array of factors are involved in the MCF innovation process, and the framework distinguishes seven categories:

- **Catalytic Factors:** Catalysts are the principal motivators of this colossal undertaking and are the sparks that ignite innovation of a more disruptive nature. These powerful factors are normally external to the MCF innovation system and their intervention occurs at the highest and most influential levels of the eco-system and can produce the conditions for enabling considerable change and disruption.
- **Input Factors:** These are material, financial, technological, human and other forms of contributions that flow into the MCF innovation system. Most of these inputs are externally sourced but can also come internally.
- **Institutional Factors:** Institutions are rules, norms, routines, established practices, laws, and strategies that regulate the relations and interactions between actors (individuals and groups) within and outside of the MCF innovation system (Edquist & Johnson, 2005, p. 46; Ostrom, 2007, p. 26). Rules can be formal (laws, regulations, and standards) or informal (routines, established practices, and common habits). Norms are shared prescriptions guiding conduct between participants within the system.
- **Organizations and Other Actors:** The principal actors within the MCF innovation system and main units of analysis of the framework are organizations, which are formal structures with an explicit purpose and they are consciously created. They include firms, state agencies, universities, research institutes, and a diverse array of organized units.
- **Networks and Subsystems:** Social, professional, and other types of personalistic networks are invaluable means for connecting actors within and beyond the MCF innovation system. Networks provide invaluable means of sharing information, often more quickly and effectively than traditional channels and they help to overcome barriers to innovation such as rigid compartmentalization that is a prominent feature of innovation systems (Taylor, 2016, pp. 157–168). Subsystems are issue or process-specific networks that link organizations and other actors with each other to produce outputs and outcomes (Weible et al., 2012; Jenkins-Smith et al., 2018). Numerous subsystems exist within the overall MCF innovation system and they can overlap or be nested with each other. The procurement and research and development subsystems are two of the most prominent subsystems.

- **Contextual Factors:** This category covers the diverse set of factors that influence and shape the overall MCF innovation environment. Contextual determinants that exert strong influence include historical legacy, domestic political environment, development levels, geographical diversity and a country's size and its markets.
- **Output Factors** are responsible for determining the nature of the products and processes that come out of the innovation system. They include the production process, commercialization, the role of market forces such as marketing and sales considerations, and the influence of end-user demand.

1. Catalytic Factors: High-Level Leadership Engagement and the RMA

Although MCF has attracted attention and support from Jiang Zemin and Hu Jintao between the early 2000s and early 2010s, much of this interest and engagement was sporadic and superficial and lacked sufficient political clout and credible commitment to overcome the difficult structural obstacles that blocked the path of meaningful progress in integrating the civil and defense economies. Xi Jinping's active and sustained interventionalist engagement in MCF affairs since 2015 is having a profound impact in reshaping the dynamics and momentum of MCF policy making and implementation.

Xi's decisive involvement in MCF can be highlighted by two events. The first was his announcement in March 2015 to elevate MCF into a national-level development strategy. Prior to this move, MCF was a sector-level industrial policy being managed by mid-level government and military officials. Xi's intervention quickly catalyzed high-level political and bureaucratic engagement. In March 2016, the Politburo approved a document titled "Opinions on Integrated Development of Economic and National Defense Building" and approved MCF as a national strategy ("Consideration of 'Opinions,'" 2016). These opinions formed the basis of the 13th 5-Year Special Plan for Science and Technology Military Civil Fusion Development that was issued in 2017 by the CSTC and MOST.

Another imprimatur of Xi's high-powered MCF involvement was his willingness to become the head of the Central Commission for Integrated Military and Civilian Development (CCIMCD) that was created in January 2017 to oversee MCF matters. Establishment of the CCIMCD was an unprecedented breakthrough with powerful Party, state, and military leaders as members.

A second important catalytic factor in promoting major development in the MCF innovation system is the global threat environment, especially technological threats and opportunities. Xi and the Chinese leadership perceive that the world is currently in the midst of a profound science and technology revolution in both the military and civilian realms and that China needs to be at the forefront of riding this change.

A focal point of this technological transformation lies in the intersection between civilian and military affairs, especially in the information and autonomy domains. These technological revolutions occur infrequently and in order to take full advantage of this opportunity and leapfrog to the global frontier, the Chinese authorities see the need to have a carefully coordinated undertaking between the civilian and military communities in areas such as artificial intelligence, big data processing, high-performance computing, advanced manufacturing, and robotics. This is being carried out in large-scale industrial and innovation initiatives such as the Made in China 2025 Plan and the Science, Technology, and Innovation 2030 Major Projects Plan.

2. Input Factors: Financial Integration

Input factors are the basic building blocks in the defense and civilian economies needed to advance the goals of MCF. They are tangible "hard innovation capabilities" and include advanced research and development facilities, firm-level capabilities in R&D and manufacturing, a cadre of experienced scientists and engineers and supporting programs to cultivate human talent, technology transfers, sourced domestically or through international knowledge markets, as well as the availability of funding and investment sources from state and non-state sources (Cheung, 2011). In the case of MCF, it also includes infrastructure projects and markets that create civil-military hybrid industrial and technological clusters. China has made large investments into building up these tangible inputs and infrastructure factors since the turn of the 21st century and this subject has received much analytical attention.

One of the most significant initiatives of the past few years has been the vast new sources of funding for the defense industry and MCF projects both through the capital markets and government venture funds. Over the past decade or more, the political and military leadership has come to grips with financial demands of achieving the goals of its expansive military modernization drive (Chaofeng, 2014). In addition, traditional forms of state funding—whether from the defense budget, subsidies and loans, or the sector's own profits—perpetuate a high degree of insulation from market forces. Greater opening to the capital markets offers the potential both for a large, new source of financing while stimulate greater accountability and competitiveness into a closed defense enterprise system. This section will focus on this subject area.

A cursory glance at the state of China's defense technological and industrial base (DTIB) serves as a useful reference point from which to assess the role of financial MCF. Measured by revenue and asset-base ($367 billion and $640 billion), the defense industry in China in gross terms is a thriving sector.[1] Importantly, however, is the rate at which the DTIB has grown in the recent past. In the past 10 years, while employee numbers have edged up only modestly, its revenue and asset base have ballooned, in several cases well over 150%, much more than its western counterparts, and an amount that could more than double again in the next five years ("The Frequent Claim," 2016).

The size and growth of the Chinese DTIB is in marked contrast to its meager performance as measured by profit growth and return on assets. Over the past five years, while all major defense enterprises have shown profits, they have been modest (averaging RMB 68 billion in the past five years), with some exceptions. More importantly, their average year-on-year growth in profits and return on investment (ROA) have been flat (<1% per annum since 2015), again with a few exceptions in the aerospace and ordnance sectors, while the overall average ROA is a mere 1.7%.[2] All in all, the Chinese defense industry, while pronounced in size and output, continues to underperform financially and contributes

[1] Data for defense industry was collected from various sources (including http://www.csindex.com.cn; http://www.fortunechina.com, http://stock.jrj.com.cn) as well as defense industry year end reports and websites.

[2] Boeing's and Airbus' average rate of profit increase for this timeframe is 19% and 47%, respectively, while their average ROAs over the same period have been 5.5% and 2.1%, respectively. See http://www.fortunechina.com/fortune500/node_65.htm and Boeing and Airbus websites.

modest profits to its own operations, raising the question of how its large and rapid expansion is being funded.

Naturally, the defense budget, and in particular the procurement budget, is a substantial source of income for the defense sector ("China's Defence Industry," 2018). However, the growth in the defense budget is slowing, reflecting a slowing in the broader economy. Financial transfers, subsidies tax breaks and especially low-interest loans have been the other sources of support and are certainly significant for state-owned enterprises—including the defense industry[3] (Haley & Haley, 2013, p. 2). While these conventional sources of funding are substantial, they do not account for the doubling in size of the defense industry during the last 10 years.[4]

Instead, the Chinese government has increasingly turned to new forms of financing to recapitalize the defense industry. These are closely linked to MCF efforts, because these defense monies are being tapped in the commercial and private capital markets. This trend was slow to develop until the passage of the mixed ownership reform initiative (MOR) in 2015 ("Opinions on Promoting Development," 2015). MOR encouraged the joint equity stakes by government and private shareholders in state enterprises, with the dual goal of expanding the defense industry's capital access and exposing the defense enterprises to greater market forces and thereby accelerating their reform. Moreover, the latest initiatives in defense sector reform have been the restructuring of research institutes, where some of the most productive assets lie. In early 2017, a pilot plan to reform 41 research institutes was confirmed ("Reform to Classification," 2017).

Mixed ownership has manifested in the markets in several important ways. First, defense securitization includes over 100 listed companies on China's primary stock market, most of which are majority controlled by the defense industry groups or other state-owned entities ("Structure and Design," 2018). These companies raised an estimated US$63 billion between 2010 and 2016 through various market operations (Cheung, 2016). Another form of defense industry participation in the market has been the rise in asset-backed securities, whereby state-owned non-liquid assets are converted into investment vehicles that can then be sold to intermediary financial institutions to be indirectly traded in primary and secondary capital markets (Yuwa, 2007).

The overall asset securitization rate of China's defense industry currently stands at an average of 33%. With a current total defense industry asset base of RMB 4.15 trillion ($638 billion), there is the potential to tap an additional several trillion RMB in the market as the defense industry opens up ("At a Rate of Only 30%," 2017). If the higher predictions of 20% annual growth in the defense industry overall for the next 5–10 years is realized, these astronomical figures may not be unwarranted, though many barriers remain to its implementation.

Another financial phenomenon that will profoundly impact the future of MCF implementation in China is the tidal wave of government guidance funds (GGFs) that has emerged on the scene in the last three to four years (Liang, 2018). GGFs are part of a

[3] One estimate put the amount of subsidies to SOEs at US$310 billion (~2 trillion RMB) from 1985–2005 (nominal terms).

[4] Between 2009 and 2018, asset value has gone from roughly RMB2 trillion to over RMB4 trillion, and revenue has gone from RMB1.4 trillion to RMB2.4 trillion.

broader state-directed industrial policy to channel national resources into its goals under its 2016 “Innovation-Driven Development Strategy” (Ministry of Science and Technology, 2016). These efforts consciously link defense and civilian production and R&D capabilities to achieve its goals. Moreover, among the now thousands of GGFs that exist, explicit MCF projects have risen as an important portfolio of many local government sponsored GGFs.

To summarize the financial landscape of MCF, these new channels of funding in the form of securitization and government guidance funds are significant both in their scale, and in their nature. They represent in aggregate the opportunity for massive financial recapitalization of China’s DTIB, but they are being tapped with limited effect on the restructuring and opening up of the defense enterprises to the civilian participation. In fact, the evidence suggests their monopoly position and political status have risen in the past few years. The nature of a state-led investment approach poses inherent contradictions for an MCF economic model that seeks a genuine participation of the civilian private and commercial sectors with the defense sector.

3. Institutional Factors: Formal and Informal

The role of institutions is of central importance to innovation systems. Broadly defined, institutions are the norms, routines, habits, established practices, and other rules of the game that exist to guide the workings of the system and the interactions between organizations (North, 1990, pp. 4–5). These come in formal (such as development strategies, laws, and standards) and informal (conventional routines, market incentives, governance norms) variants. The notion of institutions is particularly salient for China’s MCF program because of the interplay of so many actors across industrial sectors, state and market entities, central and local governments, and civilian and military agencies. Understanding the nature of interactions amongst this panoply of organizations is critical because creating an effective institutional arrangement to achieve this has been one of the most intractable challenges for the Chinese leadership in its pursuit of MCF goal of fostering an innovative and collaborative ecosystem.

Under the Hu administration, efforts to promote MCF focused primarily on reforms to defense corporations and on establishing a body of regulations, policies, standards, and other mechanisms by which to encourage the flow of private-sector technology, talent, and investment into defense projects. The work done in building up these institutions is voluminous (Wenxian et al., 2015).[5] In essence, this pre-Xi period laid the *formal* institutional foundations for MCF. What this phase failed to accomplish however, as pointed out earlier, was to fundamentally alter established social, organizational, and cultural patterns of interaction and norms of behavior (Xie & Lu, 2014). In other words, the *informal* institutions relevant to MCF have proven far more difficult to change. A lack of leadership engagement and an overarching strategy led to ad hoc, structurally misaligned initiatives (Lafferty, 2019).

From an institutional perspective, Xi altered the MCF landscape in several important ways. First of all, a raft of new high-level strategies, plans and other administrative arrangements have been developed following 2015 Xi’s decision to elevate MCF to a

[5] One compendium of these efforts details over 300 major regulations, standards, and planning documents, covering a wide range of procurement, intellectual property rights protection, and other provisions issued by a host of agencies including GAD, the CMC, the State Council, the NDRC, SASTIND.

national strategy that collectively represent a committed effort to reform the defense S&T industrial base and shift behavioral norms and practices. They build on previous ideas but are much more specific in the sectors and actors involved, and call for closer collaboration between civilian and defense sectors working in these fields ("Xi Jinping Presided," 2017). Unlike previous institutionalization of MCF, these documents are issued by a superior authority ("Bluebook on Prospects," 2019).

A second way in which Xi is altering the institutional environment is by integrating MCF initiatives with the larger innovation-driven development strategy and many of the major national S&T programs associated with it. By linking strategic plans and initiatives together, and funding resources along with it, the interaction between organizations involved in these pockets of innovation is moving toward a freer, more fluid collaboration and exchange of ideas. This is most apparent in cutting-edge technology fields with strong government support, but it is occurring spontaneously in technology centers around the country, indicating a shift in normative behavior or informal institution building (Hagt, 2019).

Similarly, through his high-tempo and wide-ranging production of laws and opinions, Xi Jinping is not just ramping up a set of formal institutions but he is also sending a strong political signal of commitment to a MCF agenda. This catalytic factor in China's MCF ecosystem is impacting the relationship of other factors, as the innovation literature predicts (Kline & Rosenberg, 1986). Xi's support for MCF is coordinated with resource allocations, which is altering the interaction of organizations and changing mindsets and conventional practices.[6] The gradual rise in enthusiasm for experimenting with MCF projects at the local level is an example of this phenomenon. Also, the publication of product catalogues and technology patents also show changes in conventional practices.

4. Organizational Factors

Organizations and other actors in the civilian and defense economies are central factors in the MCF innovation system. They are the vehicles for technological change in that they carry through and facilitate innovations (Edquist & Johnson, 2005). Collectively, organizations refer to entities that are directly or indirectly involved in supporting a MCF economy, ranging from private and defense corporations, to government agencies, military entities, and the research and development system, but can also be key individuals in the policy decision-making process. Creating a MCF ecosystem, which calls for an additional set of actors and institutions, has been difficult given the complexity of managing a much broader group of players and interests in China's political economy (Cheung, Mahnken, & Ross, 2018).[7] This section will focus on one of the critical elements catalyzing China's current MCF innovation eco-system: the CCIMCD.

The creation of the CCIMCD in 2017 under Xi's leadership was an unprecedented move and is the highest such organization in Chinese history to oversee MCF related work (General Staff Department Compilation Group, 1991, p. 567). This Party institution was necessary not only to bring together the various civilian stakeholders within the economy, but also to bridge the two major parts of the Chinese system: the State Council, China's

[6] For instance, officers from CEDD, AMS, and NDU emphasize that past MCF-related efforts were frequently resisted by local if not aligned with its interests, but sustained political attention mitigates that over time. Interviews in Beijing, 2017.

[7] These authors distinguish between defense and military innovation.

supreme executive body overseeing the civilian national economy, and the Central Military Commission, China's leading military institution. Policy practitioners of the civil-military economy in China have long bemoaned the lack of such a supra-organization (Chuanxin, 2014). Without it, coordination of these two systems of equal rank in China's body politic in the pursuit of a complex undertaking like MCF is doomed to bureaucratic inertia, as previous efforts had demonstrated.[8]

The CCIMCD is populated with around two dozen senior Party, state, and military leaders. Its importance is best represented by the fact that the body has already convened four meetings, issuing important policy guidance on MCF initiatives with increasingly more specific measures to implement MCF across the country (Guangrong, n.d.). The CCIMCD is also distinctive in that the military has substantial representation in this body with five members (members and vice-chairman of the CMC)[9] ("Han Zheng Chairs National Symposium," 2018). This is a significant point given that MCF is an initiative that involves the civilian economy, a domain traditionally (and constitutionally) off limits to the military.[10]

Civilian Actors

The State Council, a supra-agency with chief administrative authority in China, holds a number of departments and ministries responsible for MCF. Two agencies are most relevant in this respect: the National Development and Reform Commission (NDRC) and State Administration for Science, Technology, and Industry for National Defense (SASTIND). The NDRC is a core department of the State Council with wide-ranging powers over major national development projects and their funding. Within this commission is the Department of Economic and Defense Coordination, which is the body most focused on macro-level economic planning involving the defense and non-defense sectors, with particular purview over national economic mobilization. With the NDRC's prominent role over economic planning, it also takes a lead role in MCF activity and is a principal in convening meetings.

SASTIND is a relatively lower ranked body, but it is the only agency charged with directly regulating the defense enterprises.[11] It is an agency under the Ministry of Industry and Information Technology (MIIT), the large bureaucracy with a purview over industrial planning and regulation. On the surface, this makes for a rational organizational framework, bringing defense and non-defense sectors under one administrative roof.

A number of other bureaucracies have a degree of input with respect to MCF implementation, including MoST, which plays a central role in the country's vast national S&T program—including the planning of S&T parks—much of which has dual-use applications. The State-owned Asset Supervision and Administration Commission (SASAC) and its local branches manage and own state enterprises, including the defense sector. In

[8] In general, previous MCF efforts were ad hoc, structurally misaligned, of low policy priority. See Chao (2016).

[9] Previously Zhang Gaoli and currently Han Zheng.

[10] This point was made by NDRC officials. Interview BJ27-8.

[11] SASTIND has control over a substantial pot of money (estimated at RMB 100 billion over 10 year period, granted sometime in the mid-2000s), but interviewed sources generally admit that SASTIND is relatively weak and without this funding, would have little influence over the defense enterprises. Interviews in Beijing, 2015.

general, their responsibility is to ensure returns on investment of SOEs, but they also have some input in performance evaluation of state-owned sector leaders. The Ministry of Finance (MoF) is also involved with evaluating and funding development projects and supporting industry parks across the country. The State Intellectual Property Office (SIPO) is in charge of patents, intellectual property, and technology transfer in China and works with the CMC to declassify defense patents.[12]

Military Actors

The structure of leadership over MCF activity on the military side also involves a number of high-level bodies. The agency formally charged with leading this effort is the CMC Office of Strategic Planning (COSP). Originally a third-level organization subordinate to the General Staff Department, the COSP was elevated to one of the 15 departments directly under the CMC under the 2015 reforms, and is responsible for the overall configuration of defense resources and the PLA's modernization goals, particularly in science and technological innovation. An important task under this bailiwick is civil-military integration, and the department houses the MCF Bureau to manage the military's efforts and is the principal contact with State Council departments working on MCF.

Two other sources of expertise with regard to MCF reside in the PLA. One of these is the CMC Equipment Development Department (CEDD), responsible for procurement, acquisition, and defense R&D. CEDD was formerly a powerful general department, housing substantial expertise in managing defense projects, and had the closest relationship with the defense industry sector (Hagt, 2014). It has traditionally been the principal advocate for MCF in the military and supports the MCF Bureau. Another important player in MCF on the military side is the CSTC, a body also promoted in status under the 2015 reforms, reflecting the importance placed on S&T for military innovation. This institution also holds substantial expertise through its traditional relationship with military research institutes in the defense industrial base. The CSTC works with MoST to identify dual-use and MCF collaboration in key national S&T projects, the product of which was a recently published S&T MCF development plan (Tao, 2017).

Other departments involved more peripherally in MCF include the CMC Joint Staff Department (CJSD), which is in charge of operations and overall command and control of the armed forces ("The Battlefield Environmental," 2016; "The First Geology MCF," 2016). Also the Strategic Support Force, responsible for space, cyber, and electronic warfare, has built ties outside the military, signing cooperation agreements with research universities and software development companies (Laskai, 2018). The National Defense Mobilization Department—another body carved out of the former GSD and placed directly under the CMC—is significant in that defense mobilization planning dovetails with MCF efforts in a number of ways, such as the collaboration of transportation and communication infrastructure development projects to meet both civilian and military needs. In this respect, this organization works with its State Council counterpart to coordinate defense mobilization requirements. But it is also significant for its charge over the Provincial Military Commands (PMC) ("16 Provincial-Level," 2018). In short, this branch is the PLA's most direct interface with local (provincial governor) leaders on matters relevant to MCF (Li, 2014). The most

[12] SIPO works with the CMC National Defense Intellectual Property Office, and in early 2017, over 3,000 declassified defense patents were released at www.weain.mil.cn. Also, see Nouwens and Legarda (2018).

recent organizational addition to MCF relevant efforts under the CMC is the founding of the Military Science Research Steering Committee (MSRSC), an agency launched in early 2017 that is modeled on U.S. DARPA (Ni, 2017). Its specific mission is as yet unclear but will likely be to identify priority areas for investing R&D resources in both defense and civilian sectors and thereby help guide national security development plans.

There are several distinctive features of China's organizational approach to guiding its MCF strategy that point up both strengths and weaknesses in its design. With this new institution, the Party leadership has finally resolved a longstanding barrier to joint planning of the defense and civilian components of national economy and S&T innovation system. Second, the formation of a permanent commission, rather than an ad hoc leading group, sends a strong political signal about the top leadership's vision to pursue a long-term strategy of MCF.

It has led to a proliferation of institutions and planning initiatives at many levels of government.[13] The administrative and functional lines, and their status and authority in decision-making are unclear. In the State Council, for instance, the relationship between SASTIND and the MCF Promotion Bureau—both formally under MIIT—is ambiguous. The effectiveness of the NDRC and its subordinate National Mobilization office to coordinate with other offices is also problematic. On the military side, the MCF Bureau has little specific expertise and must rely on assistance from the CEDD and the CSTC, where relevant competence traditionally was housed. The addition of yet another body to guide R&D efforts in the military sphere, the MSRSC raises questions about its distinctive role in MCF, in relation to the MCF Bureau or the CSTC, both of which also have responsibilities over military R&D efforts (Grevatt, 2017). In short, the uptick in political commitment to MCF and the rise in organizations dedicated to this effort will help empower its implementation, but it will also increase bureaucratic bargaining, as China's system has frequently proven in the past (Lieberthal & Lampton, 1992; Mertha, 2008; Dougan, 2002).

A second feature evident in the organizational architecture is the limited role of the MCF strategy's foremost proponent, the military. While the PLA is substantially represented in the CCIMCD, it has virtually no footprint at the local level. This was not always the case. The PMC (*sheng jun qu*), through its role in national defense mobilization and procurement responsibilities for military region forces, had the potential to serve in some capacity as a useful local platform for certain types of MCF activity ("Following Reform," 2016; Li, 2014). However, the PMC's purview over local mobilization and army building was curtailed under the 2015 reforms, effectively constraining the potential of this regional civil-military entity as a platform for MCF. At local level, the military essentially has no direct formal representation to interact with government departments in charge of economic and industrial affairs and therefore has little authority or means to promote a MCF agenda with local development planning.

A third distinguishing feature here is the central role of the state-owned enterprises in China's defense industrial system. The 11 major defense firms control and operate the majority of China's defense sector research, development, and production. Despite ongoing reforms to transform their historically closed-off nature—through MOR reforms—the defense

[13] This discussion of continued bureaucratic chaos comes mainly from interviews with officials in 2017 and 2018 (Hagt, 2019).

industries have so far remained resistant to fundamental change (“90% of Defense Enterprises,” 2018). Moreover, their dominant position in the defense political economy arena of China’s system means that they will be instrumental in the outcome of an integrated national development plan that the MCF strategy envisions (Lafferty et al., 2013). However, there is effectively no direct authority or control over defense industry enterprise operations, and real power over them lies within the Communist Party. Since the CCIMCD has not yet been replicated at lower levels of the political system, there is a large power differential between the defense enterprises and the much lower ranking local governments in which they reside, making comprehensive planning needed for MCF difficult to achieve.

5. Networks and Subsystems

Traditional and formal organizations and institutions, many of which are described in this paper, heavily dominate China’s MCF infrastructure. In fact, the formation of government bodies and the crafting of laws, regulations and planning guidelines are a particular strength of China’s state-centric model of industrial policy making. However, as the literature makes clear, networks and subsystems are the “interstitial connectors” that link actors and processes in the innovation ecosystem and are crucial to mitigating compartmentalization and enhancing information sharing and technology diffusion (Taylor, 2016, pp. 157–168). Until recently, there has been an absence of such platforms in China’s MCF system, a product of its statist approach, and exacerbated by issues such as secrecy, historical legacy, and unclear IPRs and the monopolistic behavior of its defense firms. However, that is changing, and an exciting new development in China’s MCF efforts is the emergence of a range of novel mechanisms that are enabling these crucial linkages in the system.

Subsystem: CMI Acquisition System

One of the most prominent of these is the formation of what amounts to a new CMI-specific acquisition regime that is in part a reform of, but is also separate from, the existing monopoly-oriented system. The PLA and the State Council have instituted many components to this new acquisition platform that allow for private sector firms to be vetted and approved for defense work, that facilitate a more open bidding process and generally enhance transparency of the acquisition governance regime.

Some of the elements of this new system include web-based portals that are appearing both at the national and local levels. The much-heralded PLA’s Weapons Acquisition Information Network (WEAIN), launched in 2015, provides information on the country’s weapons and armament needs, relevant policies, procurement notices. Moreover, the PLA has vetted 13 intermediary tendering agencies to screen applicants and manage the bidding process (“The Military’s Weapons,” 2018). As of early 2018, it had attracted over 16,000 registered entities and listed more than 4,500 technology procurement notices (Yang, 2018). Moreover, the site also holds over 3,000 defense patents that were declassified in 2017 as part of an effort to increase transparency and encourage the private sector to engage defense research and production (Nouwens & Legarda, 2018). Many local governments and S&T parks have founded similar online platforms.

As of October 2017, the PLA, in conjunction with SASTIND, officially announced the streamlining of the arcane defense contractor approval process, making it substantially easier for smaller commercial firms to obtain the necessary licenses and approvals (“*Mincanjun*,” 2017). Extensive catalogues of products, technologies, and firms for researching, developing, and manufacturing military weapons and equipment were released by SASTIND.

Within the last year, a number of reforms to the tax system, the pricing of military products and technologies and standards have made substantive progress, all of which are paving the way for greater private participation in the defense acquisition system. Commercial enterprises can now enjoy many of the tax incentives previously restricted to defense firms (lower VAT and "return first policy").[14] The fixed pricing system (cost-plus) that dominated earlier eras has given way to more flexibility and includes a range of negotiable pricing schemes for a much larger portion of defense products and technologies (Xi & Bingwei, 2018).

The PLA has also increased its efforts to sidestep the traditional acquisition system, particularly with regard to accessing the private and commercial domains for high-end and emerging technologies. The newly empowered CSTC now has greater control over the early phases of the R&D process—for example, experimental and exploratory research—whereas this was overseen by the General Armaments Department prior to 2015 reforms. The previously mentioned Military Science Research Steering Committee also serves to better identify emerging technologies for military application in the private domain. The creation of the National Defense S&T Innovation Rapid Response Team under the CSTC, located in Shenzhen, is the most recent move. This is very similar to the DIUx offices in the United States and forms another part of this new system to enhance technology acquisition in the commercial sphere.

Networks: Non-Traditional Platforms

There are also novel ways in which China is generating cross-linkages in the system. First, exhibitions where civilian and military enterprises gather to show off technologies and exchange information have proliferated. The Zhuhai Airshow is the most visible of these, but virtually every major S&T center convenes these events to demonstrate new dual-use projects and burgeoning MCF areas as well as facilitate a two-way channel of communication between private and defense enterprises. SASTIND has been the leading agency in holding exhibitions, but the PLA has also shown increasing interest in directly participating ("Private Enterprise," 2014).

The designation of national MCF demonstration bases has also been a prominent strategy to foster interaction between defense and civilian activities. As of mid-2018, there were 36 such bases in 22 provinces and cities around the country (Ministry of Industry and Information Technology, 2018). These are important because underlying this strategy is the notion that spatial proximity is key to technology diffusion. Industry clustering fosters a higher degree of interconnectedness that encourages spillover in technology and knowledge—between defense and commercial firms—thus stimulating productivity and innovation (Jolly & Zhu, 2012).

One of the most novel developments in China's MCF economy is the intermediary entities that are on the rise in many local governments. These range from government to quasi- and even non-government institutions, which provide an array of liaison, research, and consulting services to facilitate information exchange and interactions between civilian and defense actors in the local economy. Such organizations are especially active in thriving economic centers where industrial and technological complementarity with the resident

[14] Interviews in Chongqing, May 2016. For discussion on tax reform, see http://pg.jrj.com.cn/acc/Res/CN_RES/INDUS/2019/3/6/4e258c51-a0d9-4eff-9517-7455fc98a073.pdf

defense industry is higher. These intermediaries are unique in that they either have experts in-house that have defense industry backgrounds, or their staff includes retired military officers familiar with defense procurement and acquisition practices.[15]

In sum, these various platforms that are making their debut in the past few years largely fall outside the conventional actors and institutions of the MCF system. Yet, they constitute a vital enabler for MCF implementation in local economies where the threshold for the majority of commercial and private enterprises is too high to engage in defense work (Huixian, 2017). They provide the connections between the notoriously separate defense and civilian parts of the economy. These emerging entities are helping generate the bottom up collaboration that will be essential if MCF is to succeed.

6. Contextual Factors: MCF Implementation

This category comprises a set of conditions that shape the environment in which MCF happens. In this sense, they are usually broader in scope than other factors (such as inputs and formal organizations) and cover political, institutional, and even ideational aspects of an innovation system (Abramovitz, 1986). Using the framework of contextual factors is especially useful when examining China's MCF efforts at local levels, where much of the implementation occurs. The complexity of China in terms of geographical diversity, levels of development, governance structures and historical legacies dictate that MCF will be carried out with a high degree of variance in form and substance. And the aggregate of these contextual factors help understand the specific operating environment of MCF and the different outcomes that it leads to.

The set of conditions that impact MCF implementation can be summarized under several overarching variables, which, while not comprehensive, aid in deriving general models and are important indicators of their relative success (Hagt, 2019). The first is what may be called complementarity between the local economic and political context and the resident defense entity. In order for collaboration between the defense and commercial sectors to occur, a local economy must be sufficiently competent (in either industrial or technological aspects) in providing what the defense sector requires; or vice versa, for the defense sector to integrate with the local economy, it must be able to produce goods and technologies the commercial sector demands.

A second variable that is unique to China's system is the role of center-local relations. The objectives of a national MCF strategy are not always aligned with local development priorities and properly structuring incentives for civil-military collaboration is almost without exception a difficult center-local exercise. The center-local dynamic is also manifested in other ways. China's political system is sensitive to rank and status within the party and government structures. This hierarchy of power and position comes to be an important factor for MCF implementation because the defense industrial enterprises, as central, monopolistic institutions with immense influence at the political Center, are difficult to manage by local officials who are much lower in status.

A final variable affecting MCF implementation is the notion of governance. In general terms, this is the local government's ability to mobilize and effectively utilize its natural, financial, economic and political resources to pursue a policy agenda—in this case, MCF. In other words, how well a local government can parlay its particular economic and industrial

[15] Interviews in Shenzhen and Beijing, 2016–2017.

strengths into effective implementation of MCF has an important governance dimension. These variables interact dynamically across the national landscape and shape the implementation of MCF in myriad ways. This complexity at the national level does not lend itself easily to gross assessments; however, there are three relatively coherent models of a MCF economy that can be identified.

7. Output Factors: Measuring Implementation

Output in the context of defense innovation and the systems innovation literature is broken down into a number of archetypes, ranging from simple copying at the one end to sophisticated disruptive innovation at the other (Cheung et al., 2018). The notion of output for a MCF economy must differ to an extent because one is not just looking at technological innovations, but the level of collaboration and integration between the civilian and defense sectors that generated the output. In other words, the relational dimension of the civil-military axis is decisive.

There are many forms of civil-military activity conducted around the country that fall under the larger rubric of MCF. If conceptualized along a continuum, higher value types of MCF reflect closer collaboration and lead to greater efficiency and innovation gains in the system but they also become more challenging politically as an increasing array of organizations and institutions become involved. These extend from simple defense conversion with little or no integration on the one extreme to organic fusion of defense and civilian economies on the other. The current state of MCF is the widening participation of the commercial and private sector in the defense economy (*mincanjun*), though primarily lower (3rd and 4th tier) component supply in addition to discrete, or stand-alone technologies.[16] Quantifying MCF along this value chain is a direct way to measure output of a MCF innovation system.

The problem in measuring MCF output based on this formulation is a paucity of data. A second difficulty is the lack of specificity in documenting the nature of MCF conducted. This is partly for a lack of commonly held standards when reporting MCF s, but many local governments and agencies that benefit from “MCF output” are also incentivized to exaggerate results. Many cities and provinces use crude methods of calculating “MCF degree,” which are devoid of significance in both qualitative and quantitative terms (“Speech by Luo Qiang, Mianyang Party Secretary and Cao Zhiheng,” 2014).

That is not to say that all data published by the government are meaningless. Many government and military agencies provide some quantification, but these are usually top-line figures. For instance, one report states that two-thirds of enterprises approved to do defense work are civilian and a third of those are private firms. The PLA reported recently that by the end of 2017, almost 10,000 firms and over 700 high-tech firms had “entered the ranks of national defense and military construction” (Maorong, 2019). These headline numbers are impressive on the one hand, but they represent a miniscule percentage of their respective totals. These figures quantify civilian participation in the defense sector (*mincanjun*) in the most macro sense, but there is no discussion of quality, such as information that would help

[16] To date, expos around the country have typically showcased discrete technologies—though increasingly impressive—to sell as stand-alone systems, such as robots, 3D printing, energy storage systems, electronics, navigation equipment and software, cyber security system, high-performance materials, and drones (UAVs). See Guoli (2018).

one gauge an enterprise's engagement with the defense sector—R&D, production, design, subsystems, or component off the shelf sales.

Other, indirect quantitative methods of measuring output are also possible (Jaffe et al., 1993). One proxy for civil-military integration is technology diffusion. Joint patent activity and joint science and technology paper publications between these actors are frequently utilized to study collaboration in Beijing's innovation economy. Other ways of examining knowledge flow and technology diffusion include the use of patent citation analysis. Although much of the registered patented technology falls into the dual-use realm, all of these methods are imperfect yardsticks, as much of the data is not specifically defense oriented, or subject to selection bias (Nouwens & Legarda, 2018).

A more fruitful approach to measuring MCF progress and impact is qualitative in nature and borrows from the U.S. defense industry concept of the lead system integrator (LSI) (Gansler et al., 2009). Viewing MCF's success through this lens highlights the importance of many of the factors discussed in the systems innovation framework. A Chinese LSI from the private, corporate sector would represent a disruptive innovation at the institutional, political, bureaucratic, and economic level. Given the powerful position of the defense conglomerates, discussed earlier, the presence of an outside system integrator would clearly indicate a high level of political support by the leadership. Moreover, LSI would demonstrate genuine change in the monopolistic position of the defense enterprises and a more effective institutional and governance regime to implement collaboration.

A range of fields in high-tech, disruptive technologies where China is seeking to become globally competitive is receiving increasing analytical attention (Ray et al., 2016; Kania, 2017; Katwala, 2018; Fisher, 2010; Sinko, 2017; Krekel, Adams, & Bakos, 2012). These range from robotics, to artificial intelligence, quantum computing, aerospace, nanotechnology, new materials, drones, high performance computing, and others. In many of these, the private corporate sector is beginning to engage seriously in MCF through technology contribution, co-licensing, and partnerships in R&D ("Baidu Establishes," 2017). It is clear the military and defense sectors are able to leverage significant amount of technology and know-how from these projects. What is less understood is the degree to which firms are actively participating in these MCF projects or acting as system integrators. Government R&D institutions such as the Chinese Academy of Sciences, and defense enterprises, such as China Electronics Technology Group, continue to play central roles. Beyond these specialized technology programs, with their high-level government attention and funding, private enterprises' role in defense programs is limited to lower tier component supply. Measuring the level of participation would require deeper corporate profiling.

Implications for the United States

A central goal of China's MCF strategy is to develop and acquire weapons "better, cheaper, faster." The trajectory of that effort will have far-reaching consequences for the United States' ability to manage the military balance with China. The defense industrial complex itself has since the turn of the century greatly improved in its own ability to produce more advanced weaponry. Moreover, state-directed and funded institutions, especially Academies of Science and Engineering, national labs, and defense universities, and to a lesser extent civilian universities, represent an important *civilian* body of capabilities that have certainly helped transform China's research, development, and acquisition system. But all the available evidence strongly suggests this has come at a high cost. In aggregate, this state-led defense and civilian sectors capture enormous amounts of national resources, but these are highly inefficient (Liu, Simon, Sun, & Cao, 2011; "Interpret 'Made in China 2025,'" 2015). In short, the system has become better and faster, but not necessarily cheaper. The fact that MCF has been elevated to a national strategy with a sense of urgency precisely at a period when China is making huge strides in its military modernization suggests the leadership views a fix to the inefficiency of the system as essential to sustain this trajectory. However, the goal to fix this—facilitate the participation of China's robust private or commercial economy in defense building—has only begun to achieve results, and its prospects for successful implementation remain highly uncertain despite its high level attention at the Center. Private and commercial sector engagement in defense acquisition and procurement programs remains limited largely to 3rd and 4th tier component production. The emergence of a genuinely private or commercial entity that acts as lead system integrator for a major defense program would demonstrate deeper reform of the system. That has not yet happened, as the defense enterprises remain largely resistant to fundamental change.

Another important goal of MCF is financial integration. Asset securitization and the ability to tap financial markets represent an important turning point for the defense industrial base. Access to the market is allowing for a massive recapitalization of the defense industry. A much larger windfall of capital in the years ahead could well materialize as SOE reform moves forward. The expansion of the defense sector in the last decade attests to this increased capture of national resources through the market. This financial aspect of MCF is significant because it falls outside conventional understanding of the resources devoted to China's defense industrial base. It is not a well-understood phenomenon, in large part due to the opaque nature of China's statist market and the complexity of SOE reform. But it is certain to be an important factor in China's military modernization drive. Military procurement budgets, preferential tax treatment, subsidies and loans—all of which are slowing in growth—may not be the biggest determinants of the defense industry. Assessments of China's military modernization trajectory based principally on budgetary and extra-budgetary state largesse misses this new source of funding that will grow in size and importance over time.

Ironically, this aspect of financial integration stands in contrast to the previously discussed MCF goal of increasing innovation and efficiency of defense work through private and commercial sector participation. Ideally, SOE reform and asset securitization is meant to diversify ownership in order to infuse better corporate management and governance, not just increase resources. However, despite the substantial securitization of defense assets, the group corporations remain completely state-controlled, and even its listed subsidiaries are in the main still government owned. In other words, the financial markets are being leveraged to recapitalize the defense sector with little impact on their political or monopoly position in the economy—and in fact may be helping to further consolidate it (Milhaupt & Zheng, 2016). The implications here are that military modernization may continue apace despite the lack of progress in MCF in terms of commercial participation. The rise of government industry guidance funds, an equal and possibly larger source of capital, may only accentuate this trend.

While the narrower definition of MCF has direct implications for the state of China's defense industrial base, there is also a broader conceptual goal for the national MCF plan that has profound implications for U.S. national security and its economic relations with China. IDDS explicitly formulates an agenda that closely links defense building with nation building, blurring the lines between defense and civilian domains (Levesque & Stokes, 2016). Strategic industries and dual-use technologies are targeted for development with the aim of transforming China into a world-class power in economic, technological, and military terms. This mobilization of national resources to achieve economic-hard power makes China a techno-security state. This has obvious and direct implications for America's own defense industrial base, but even more troubling are the indirect, less discernible risks to U.S. defense and economic superiority.

The broader challenge for the United States regarding China's MCF strategy is two-fold. The first is the nature of many emerging technologies and industries from a dual-use standpoint, some of which have direct and clear defense applications—such as robotics and semiconductors—but many others that have potential for or are foundational to defense purposes that are frequently more remote from or are embedded in a long component defense industrial supply chain—specialized machine tools, artificial intelligence, and biotech are examples here. Moreover, most of these technologies have vast commercial potential, which means they are available to anyone and their development is widespread, making their monitoring for national security purposes a highly complex undertaking. The second and interrelated challenge stems from China's own well-defined industrial strategy linking defense and civilian economic goals, and which directly influences both outbound and inbound FDI. This intrinsically dual-use development plan entails the targeting of technologies and industries much farther upstream and downstream in the supply chain—both defense and commercial—than would normally be the case (Humphries, 2015, pp. 4–6; Bureau of Industry and Security, 2016, p. 3; Interagency Task Force, 2018). Similarly, the risks to technologies and components in the defense industrial supply chain become more widely spread and so much harder to map (Brown & Singh, 2018). Taken together with the variety of financing vehicles (acquisitions, mergers, but also minority stake ownership) that are employed by Chinese investors, monitoring is extremely difficult.

To date, the tools used by the U.S. government and Department of Defense are limited, though they have improved recently with the increased attention to Chinese investment behavior in the United States. The Committee on Foreign Investment in the U.S. (CFIUS) is one of the few mechanisms in place today with real power to govern inbound investments with potential national security threat (Jackson, 2018). While originally a blunt tool that only reviewed relevant transactions that resulted in a foreign controlling interest, CFIUS' jurisdiction has recently been expanded under the Foreign Investment Risk Review Modernization Act (FIRRMA) to cover non-controlling foreign interests in critical infrastructure, critical technologies, or sensitive personal data, including via indirect investment and if a foreign government is involved.[17] Importantly, however, a radical move to include U.S. outbound investments to China with potential national security implications was removed from the final FIRRMA reforms (Donnan, 2018).

Perhaps the most important lesson for the challenge that China's MCF strategy poses for the United States has to do with political will. China's strong, centralized, state-led system allows for a substantial degree of engineering of industrial and economic goals. Such a state-centric design in industrial policy is unfamiliar to the U.S. free-market system. Even control over broad technology in the United States is highly controversial within the commercial technology community, where the largest markets for many foundational and emerging technologies are non-defense in nature. Despite the reforms to CFIUS or other tech transfer measures, several major recent studies argue that the United States remains

[17] FIRRMA takes the "direct" out of foreign investment review. Therefore other investment types (assets purchased from bankruptcies, or the presence of Limited Partners in a VC fund) can now trigger CFIUS action. Also, filings involving foreign governments are mandatory. See Croley et al. (2018) and Oleynik et al. (2018).

vulnerable to loss of critical technologies. It is unclear how the U.S. polity could muster the political will to take a whole of government approach and institute a comprehensive policy tool set necessary to protect against the depth and breadth of the challenge: from supply chain vulnerabilities, to targeted investments for tech transfer and industrial espionage. Yet, bold action may be the only means to meet the challenge of protecting U.S. military technological advantage.

References

16 provincial-level armored standing committees, nearly half of them are commanders. (2018, January 8). *Beijing News*.

90% of defense enterprises cannot access commercial capital: If defense business is so good, why isn't capital willing to invest? (2018, August 6). *TaiFangwu.* Retrieved from https://mp.weixin.qq.com/s/QhkACdCCY_bb1q7HqnJw8w

Abramovitz, M. (1986). Catching up, forging ahead, and falling behind. *Journal of Economic History, 46*(386).

Alderman, D., Crawford, L., Lafferty, B., & Shraberg, A. (2014). The rise of Chinese civil-military integration. In T. M. Cheung (Ed.), *Forging China's military might: A new framework for assessing innovation.* Baltimore, MD: Johns Hopkins University Press.

At a rate of only 30%, there is room for 3 trillion RMB in defense industry asset securitization market. (2017, December 6). *Securities Daily*. Retrieved from http://finance.sina.com.cn/stock/hyyj/2017-12-06/doc-ifypikwu1287736.shtml

Baidu establishes National Engineering Lab of Deep Learning Technology and Application. (2017, February 20). *China Youth Daily*.

The Battlefield Environmental Protection Bureau of the Joint Staff Department visit Ubinav Company (2016, December 3). *Xinhuanet*. Retrieved from http://ubinavi.com.cn/page85?article_id=22

Bluebook on the prospects for MCF development in 2019. (2019, January). *Scidi*. Retrieved from http://www.ccidwise.com/uploads/soft/181220/1-1Q220153F5.pdf

Brown, M., & Singh, P. (2018, January). *China's technology transfer strategy*. Silicon Valley, CA: Defense Innovation Unit Experimental Report.

Bureau of Industry and Security, Department of Commerce. (2016). *U.S. strategic supply chain assessment: Select rare earth elements*. Washington, DC.

Chao, D. R. C. (2016, June). Exploration of practice and theory of New China's defense industry moving toward deepening development of civil-military integration. *China Conversion, 6*.

Chaofeng, H. (2014). *Research in strategic emerging industry civil-military integration development*. Beijing, China: National Defense University Press.

Cheung, T. M. (2011, June 7). The Chinese defense economy's long march from imitation to innovation. *Journal of Strategic Studies, 34*(3).

Cheung, T. M. (2016, March 16). *Climbing the innovation ladder: Reforming China's defense science and technology system for higher-end innovation*. Workshop on Change, Continuity in Chinese Defense, Science, Technology and Innovation, Washington DC.

Cheung, T. M. et al. (2016, July 28). Planning for innovation: Understanding China's plans for technological, energy, industrial and defense development. *IGCC*.

Cheung, T. M., Mahnken, T. G., & Ross, A. L. (2018, May). *Assessing the state of understanding of defense innovation* (SITC Research Briefs).

China's Defence Industry. (2018, September 7). *Jane's World Defence Industry.*

Chuanxin, Y. (2014). *Reflections on top-level design for MCF development*. MCF Development Strategy. Beijing, China: Higher Education Press.

CMC Science and Technology Commission and Ministry of Science and Technology. (2017, September 26). *13th Five-Year Special Plan for the Development of Military Civil Fusion*. Retrieved from http://www.aisixiang.com/data/106161.html

Consideration of "Opinions on integrated development of economic and national defense building" and "Outline for Yangtze Economic Belt Development Plan." (2016, March 26). *People's Daily*. Retrieved from http://paper.people.com.cn/rmrb/html/2016-03/26/nw.D110000renmrb_20160326_2-01.htm

Croley, S. et al. (2018, October 10). How FIRRMA changes the game for tech co.s and investors. *Law 360.*

Decision of the CPC Central Committee on several major issues concerning the comprehensive deepening of reforms. (2013, November 12). Third Plenary Session of the 18th CPC Central Committee. Xinhua News Agency.

Donnan, S. (2018, May 15). Senators ditch plan to review US outbound investment. *Financial Times.*

Dougan, M. (2002). *A political economy analysis of china's civil aviation industry*. New York, NY: Routledge.

Edquist, C., & Johnson, B. (2005). Institutions and organizations in systems of innovation. In C. Edquist (Ed.), *Systems of innovation: Technologies, institutions and organizations*. Oxford, England: Routledge.

The first Geology MCF Development Forum is held in Beijing. (2016, April 27). *Xinhuanet*. Retrieved from http://www.xinhuanet.com/mil/2016-04/27/c_128937375_2.htm

Fisher, R. D. (2010). *China's emergent military aerospace and commercial aviation capabilities*. Washington, DC: U.S.–China Economic and Security Review Commission.

Following reform, PMC placed under new Department of the CMC, major general explains major tasks. (2016, March 11). Retrieved from http://mil.sohu.com/20160311/n440069952.shtml

The frequent claim of a multi-trillion defense industry market is tempered by the low precision in investment. (2016, June 1). Retrieved from http://finance.qq.com/cross/20160601/8ZLt7M88.html#0

Gansler, J. et al. (2009, January). *The role of the lead system integrator*. University of Maryland School of Public Policy.

General Staff Department Compilation Group (Ed.). (1991). *Biography of He Long*. Beijing, China: PLA Publishing House.

Grevatt, J. (2017, July 27). China sets up agency to lead military R&D. *Jane's Defense Industry*.

Guangrong, Y. (n.d.). Significant practices of MCF development since reform and opening up. *Yangshan Zhiku*. Retrieved from http://www.siss.sh.cn/kyxs/yjsy/556452.shtml

Guoli, L. (2018, October 11). Thousands of exhibits unveiled at 4th MCF High-tech Equipment Achievements Exhibition. *Xinhua.net*. Retrieved from http://www.xinhuanet.com/mil/2018-10/11/c_1123546350.htm

Hagt, E. (2014). The General Armament Department's Science and Technology Committee. In T. M. Cheung (Ed.), *Forging China's military might: A new framework for assessing innovation.* Baltimore, MD: Johns Hopkins University Press.

Hagt, E. (2019, August). *China's civil-military integration: National strategy, local politics* (Doctoral dissertation). Forthcoming.

Hagt, E. (2019, August). *MCF: National strategy, local politics* (Doctoral dissertation). Forthcoming.

Haley, U. C. V., & Haley, G. T. (2013). *Subsidies to Chinese industry: State capitalism, business strategy, and trade policy*. London, England: Oxford University Press.

Han Zheng chairs national symposium on the work of the CCIMCD. (2018, October 29). *Xinhuashe.* Retrieved from http://www.gov.cn/guowuyuan/2018-10/29/content_5335476.htm

Huixian, J. (2017, June). Innovative path to deepening development of civil-military integration. *People's Tribune*.

Humphries, M. (2015, March 20). *China's mineral industry and U.S. access to strategic and critical materials: Issues for Congress*. Washington, DC: Congressional Research Service.

Interagency Task Force. (2018, September). *Assessing and strengthening the manufacturing and defense industrial base and supply chain resiliency of the United States* (Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806).

Interpret "Made in China 2025": The task is arduous and urgent. (2015, May 19). Retrieved from the MIIT website: http://www.miit.gov.cn/n11293472/n11293832/n11294042/n11481465/16595213.html

Jackson, J. K. (2018, July 3). *The Committee on Foreign Investment in the United States (CFIUS)*. Washington, DC: Congressional Research Service.

Jaffe, A. B. et al. (1993). Geographic localization of knowledge spillovers as evidenced by patent citations. *Quarterly Journal of Economics, 108*.

Jenkins-Smith, H. C., Nohrstedt, D., Weible, C., & Ingold, K. (2018). The Advocacy Coalition Framework: An overview of the research program. In C. Weible (Ed.), *Theories of the policy process*. Routledge.

Jingjing, B. (Ed.). (2016). *Civil-military integration development report*. Beijing, China: National Defense University Press.

Jintao, H. (2012, November). *Report to the Eighteenth National Congress of the Communist Party of China*. Xinhua News Agency.

Kania, E. (2017, November). *Battlefield singularity: Artificial intelligence, military revolution, and China's future military power.* Center for a New American Security.

Katwala, A. (2018, November). Why China's perfectly placed to be quantum computing's superpower. *Wired.*

Kline, S., & Rosenberg, N. (1986). An overview of innovation. In *The positive sum strategy*. Washington, DC: National Academy Press.

Krekel, B., Adams, P., & Bakos, G. (2012). *Occupying the high ground: Chinese capabilities for computer network operations and cyber espionage*. Washington, DC: U.S.–China Economic and Security Review Commission.

Jolly, D., & Zhu, F. (2012, September). Chinese S&T Parks: The emergence of a new model. *Journal of Business Strategy, 33*(5), 4–13.

Lafferty, B. (2019). Civil-military integration and PLA reforms. In P. Saunders et al. (Eds.), *Chairman Xi remakes the PLA: Assessing Chinese military reforms.* Washington, DC: National Defense University.

Lafferty, B. et al. (2013, January 13). *China's civil-military integration* (Study of Innovation and Technology in China Research Brief). IGCC.

Laskai, L. (2018, April). Civil-military fusion and the PLA's pursuit of dominance in emerging technologies. *China Brief, 18*(6).

Levesque, G., & Stokes, M. (2016, December). *Blurred lines: Military-civil fusion and the "going out" of China's defense industry*. Pointe Bello Report.

Li, W. (2014, July 28). China's National Defense Leaderships Management System. Retrieved from http://www.china.com.cn/guoqing/2014-07/28/content_33079137.htm

Li, W. (2014, July 28). What is China's National Defense Leadership Management System? *Chinanet.*

Liang, J. (2018, December 14). GGFs: 12 trillion difficulties and contradictions. *Central Bank Observer*. Retrieved from https://m.gelonghui.com/p/226196

Lieberthal, K., & Lampton, D. L. (1992). *Bureaucracy, politics, and decision making in post-Mao China, Vol. 14*. Berkeley, CA: University of California Press.

Liu, F.-C., Simon, D. F., Sun, Y.-T., & Cao, C. (2011). China's innovation policies: Evolution, institutional structure, and trajectory. *Research Policy, 40*(7), 917−931.

Maorong, D. (2019, January 3). Opportunities and challenges of civilian participation in defense. *PLA Daily.*

Mertha, M. (2008). *China's water warriors: Citizen action and policy change*. Ithaca, NY: Cornell University Press.

Milhaupt, C. J., & Zheng, W. (2016, January). *Why mixed-ownership reform cannot fix China's state sector* (Paulson Institute Report).

The military's weapons and equipment procurement beginning the implementation of the bidding agency system. (2018, July 5). Retrieved from http://jundui.caigou2003.com/shipin/3232671.html

Mincanjun, three approvals of the defense sector. (2017, November 17). *Lanhai Changqing Thinktank.* Retrieved from http://www.sohu.com/a/204839645_100044418

Ministry of Industry and Information Technology. (2018, July). National MCF demonstration bases: Comprehensive material. Retrieved from http://www.ecorr.org/news/industry/2018-07-02/169431.html

Ministry of Science and Technology. (2016). Outline of the National Strategy of Innovation–driven Development Background Briefing. Retrieved from http://www.china.com.cn/zhibo/zhuanti/ch-xinwen/2016-05/23/content_38515829.htm

Ni, A. (2017, July 28). China reveals new military technology agency. *The Diplomat.*

North, D. (1990). *Institutions, institutional change and economic performance*. Cambridge, England: Cambridge University Press.

Nouwens, M., & Legarda, H. (2018, January 18). *China's declassification of defense patents: Novel but not (yet) a game changer* (The International Institute for Strategic Studies Report).

Oleynik, R. et al. (2018, August 18). FIRRMA expands CFIUS jurisdiction in 2 major ways. Holland & Knight LLP. Retrieved from http://www.hklaw.com

Opinions on promoting the development of mixed-ownership economy. (2015). State Council. Retrieved from http://www.gov.cn/zhengce/content/2015-09/24/content_10177.htm/

Ostrom, E. (2007). Institutional rational choice: An assessment of the institutional analysis and development framework. In P. A. Sabatier (Ed.), *Theories of the policy process* (2nd ed.). Boulder, CO: Westview.

Private enterprise high-tech achievement exhibition, Fan Changlong Xu Qiliang attends. (2014, May 29). *People's Daily.*

Ray, J. et al. (2016, October). *China's industrial and military robotics development*. U.S.–China Economic and Security Review Commission.

Reform to classification of defense research institutes has been issued. (2017, January 11). Retrieved from http://news.cnstock.com/news,bwkx-201701-4002072.htm

Sinko, P. (2017, March). State of nanotechnology R&D in China: Implications for future U.S. competitiveness.

Speech by Luo Qiang, Mianyang Party Secretary and Cao Zhiheng, MIIT's MCF Promotional Office at Mianyang's, Second S&T City International Exhibition on Science and Technology-Forum Proceedings. (2014, October).

Structure and design of defense industry asset securitization. (2018, March 15). Retrieved from http://www.sohu.com/a/225643939_778083

Tao, Z. (2017, August 23). China to boost military-civilian integration in sci-tech. *Xinhuanet.* Retrieved from http://eng.chinamil.com.cn/view/2017-08/23/content_7728310.htm

Taylor, M. Z. (2016). *The politics of innovation*. Oxford, England: Oxford University Press.

Weible, C., Heikkila, T., deLeon, P., & Sabatier, P. (2012, March). Understanding and influencing the policy process. *Policy Sciences, 45*(1).

Wenxian, T. et al (Ed.). (2015, December). *China military and civilian integration development and achievements yearbook.* MCF Equipment Technology Research Institute.

Xi calls for deepened military-civilian integration. (2018, March 12). Xinhua.

Yuwa, W. (2007). Asset-backed securitization in China. *Richmond Journal of Global Law & Business*, *6*(3).

Xi Jinping presided over the plenary meeting of the MCF Commission. (2017, June 20). *Central Net.*

Xi, Z., & Bingwei, W. (2018, October 8). *A brief discussion on the pricing of military products in private enterprises—A probe into the price of MCF products*. Paper at the Fourth MCF Development and Technology Achievement Conference and Exhibition. Retrieved from https://mp.weixin.qq.com/s/2CoJAsj5vZdqHmA8P3aeug

Xie, Y., & Lu, Z. (2014, June). Research on boundaries of the defense industry in civil-military integration. *Science & Technology Progress and Policy.*

Yang, D. (2018, January 13). Three year review of the weapons and equipment acquisition information network on the MCF road. *PLA Daily*.

Department of Defense Emerging Technology Strategy: A Venture Capital Perspective

James Cross—The Atlantic Council

Abstract

The purpose of this paper is to assess the DoD's efforts to access new sources of innovation through engagement with venture-backed emerging technology companies by analyzing dual use venture funding flows. The intended audience is threefold: DoD innovation policy makers, members of innovation units deployed to emerging tech ecosystems, and their overseers and financial backers in Congress.

The first section analyzes five years of dual use venture funding activity. The encouraging conclusion is that, at least on the surface, DoD efforts have been successful: Venture funding to dual use companies the last five years has tripled from around $5 billion to nearly $15 billion. However, a deeper look shows that the DoD overly focuses on the Early Stage segment of the market. The corresponding geographic analysis of venture flows in 2018 also shows an incomprehensible lack of engagement in Silicon Valley.

The second section lays out a multi-stage throughput model for dual use venture activity. A better familiarization by innovation leaders will effectively calibrate policy, capital, and personnel to the venture market, driving stronger outcomes for the warfighter. The third section offers a set of metrics detailed at each VC funding stage to assess the effectiveness of DoD innovation engagement.

Preface

It is generally accepted that the United States has entered a new geopolitical phase that equates to a Digital Arms race, primarily with China. Silicon Valley conceptually stands at the front lines. Whoever harnesses the newest technology for geoeconomic purposes wins. So, it would seem natural then that the DoD would send "soldiers to the front" to secure these new technologies for the warfighter.

To that end, a four-star COCOMM commander met with a group of 20 dual use VCs early in 2019 to explore commercial space options for his new multi-decade modernization program. Thirty minutes into the meeting, it became apparent, however, that no one in the room had seen his Broad Area Announcement calling for emerging tech ideas—no one, that is, except the VC rep from a prime contractor.

Four-star generals aren't the best choice for foot soldiers in this new digital conflict. The DoD needs a better strategy.

Introduction

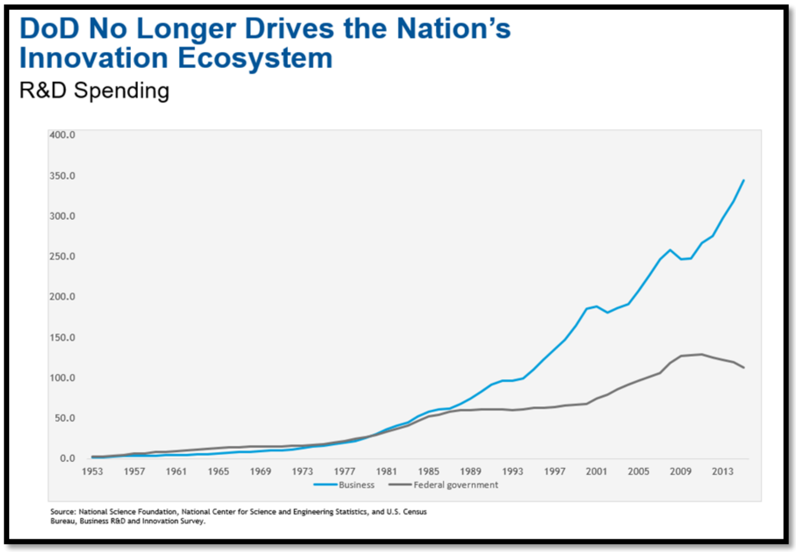
The DoD has officially shifted focus from counter-terrorism (CT) to Great Power Competition (GPC), as described most prominently in the Trump Administration's 2018 National Defense Strategy: "Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security" (DoD, 2018). Observers such as the media, industry analysts, and academics have begun talking about the new "Digital Arms Race" with China, or the new "Cold War II" with Russia and China. "U.S. Scrambles to Outrun China in New Arms Race," proclaimed the New York Times newspaper headline on January 27, 2019 (Sanger et al., 2019). Defense leaders speak of the digitization of warfare. The three traditional domains, Air, Sea, and Land, have now been expanded to the realms of

Space, Cyber, and Information. The Russians refer to the latter as “hybrid warfare,” a term trumpeted by General Gerasimov, Russia’s chief of the General Staff (Baig, 2019).

Recent DoD strategy documents decry a “digital gap” that has emerged between the United States and its adversaries in these new domains. A variety of efforts have begun to work towards closing that digital gap. Much of these efforts center around improving defense innovation and strengthening the National Security Innovation Base. Policy statements, new budget authorizations, and the development of novel DoD innovation outreach units are all aimed at accelerating the closure of this perceived gap.

The implied goal of these efforts is to better facilitate the United States in its competition with its Near Peer competitors by developing new sources of emerging technology. Secretary Mattis described this goal succinctly at the 2018 Reagan Defense forum: “Our will to win is not more important than our will to prepare to win. This includes warfighting excellence from our military, steady predictable funding from Congress, and engaged support from our most innovative industry leaders, including Silicon Valley” (Mattis, 2018).

Mattis’ statement begs the question, then, what exactly is “Emerging Tech;” with a $60 billion R&D budget, why does the DoD need it; and how does the DoD get more of it from Silicon Valley?


DoD No Longer Drives the Nation’s Innovation Ecosystem

R&D Spending

Source: National Science Foundation, National Center for Science and Engineering Statistics, and U.S. Census Bureau, Business R&D and Innovation Survey.

Figure 1. **DoD No Longer Drives the Nation’s Innovation Ecosystem**

The two most likely new sources, then, would be tech developed by the new “Tech Titans,” such as Google, Amazon, and Facebook and/or early stage emerging technology companies backed by venture capitalists. These two sources could reasonably be lumped into the DoD’s rhetorical innovation category of “Silicon Valley” given either their geographic HQ locations and/or their sources of funding originating from Sand Hill Road (the geographic center of the vast preponderance of tech venture capital).

So, the DoD is deploying resources, in terms of “boots on the ground” and dollars, to access these sources of emerging tech that their current/traditional sources of technology don’t offer through the establishment of new innovation units such as the DIU, AFWERX, and Army Futures Command (AFC). From the standpoint of a defense technology venture investor based in Silicon Valley, these units’ strategy and mission are obvious. Defense innovation policy makers are less sure of these units' mission and strategy. This is obvious considering, for example, that the DIU has had three executive directors in two years (four if you count the acting executive prior to Mike Brown [Elias, 2018]) and seen its funding cut multiple times by the appropriation committees (Williams, 2018).

From a Silicon Valley investor standpoint, the DoD should drive forward on three lines of effort to effectively engage venture-backed emerging technology companies:

1. Startups: To inspire potential founders to quit their day jobs and start that company they always dreamed of. Also, to develop an initial business model that includes selling to the government (dual use).
2. VC Funding: To help attract venture capital towards these dual (or single) use start-ups across all stages, sectors, and geographies.
3. Policy: To drive policy changes that enable the services to be more effective consumers of these new technologies at each start-up lifecycle stage with the ultimate goal of getting Late Stage emerging tech companies on Programs of Record (or the R&D/O&M equivalents).

2014–2018 Dual Use Venture Fund Flows

The effectiveness of DoD innovation engagement is difficult to measure qualitatively. The various outreach units act in an uncoordinated (and often conflicting) manner; no unit has a clear national leadership role, funding levels for the various units are inconsistent, and the uniformed services have yet to fully get involved. Quantitative measurements are much easier. A survey of publicly available venture funding in dual use categories shows that despite the DoD's miscalibrations, it is succeeding in attracting private capital. Figure 2 shows the excellent growth in dual use funding over the last five years.[1]

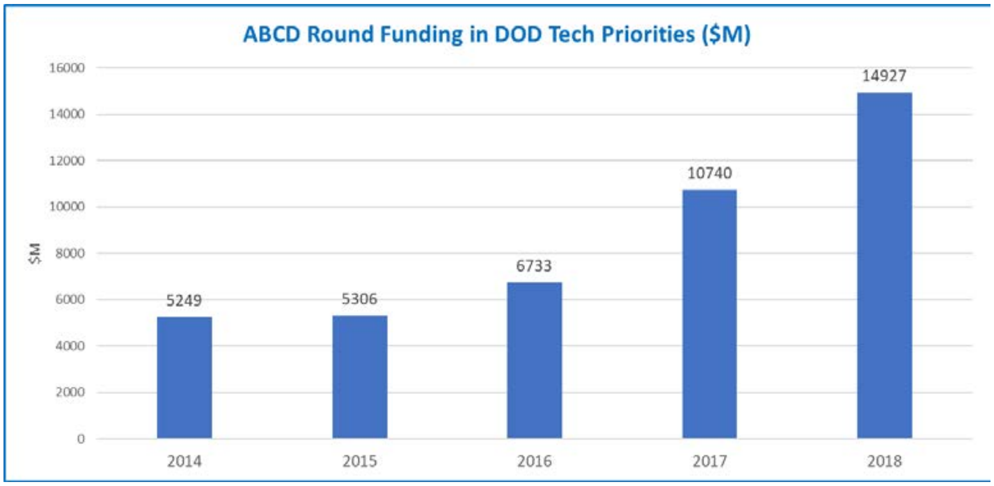


Figure 2. **ABCD Round Funding in DoD Tech Priorities**

[1] Unless noted, all venture funding data is sourced from Pitchbook with full documentation in the reference list.

Also encouraging is that the DoD has roughly held its share of VC funding steady at around 20% (see Figure 3).

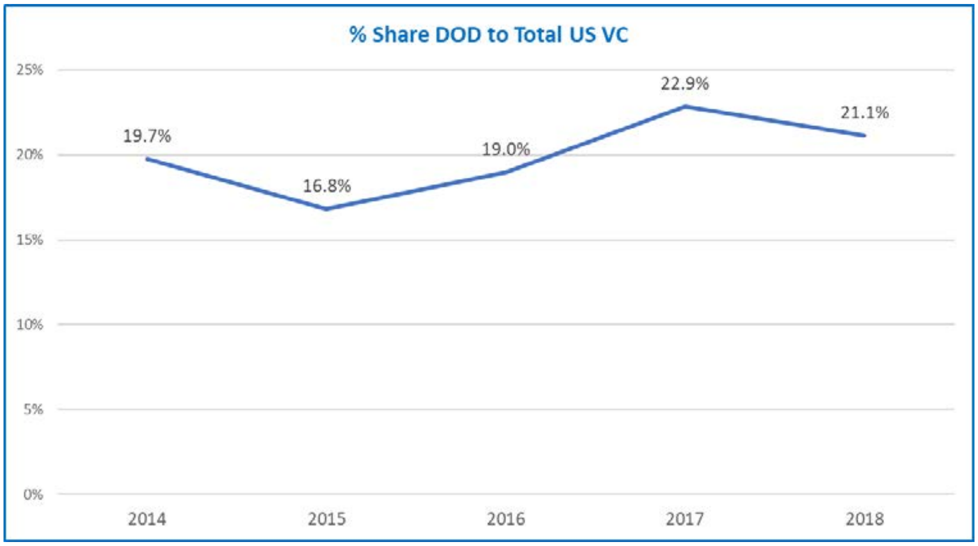


Figure 3. **Percentage Share of DoD to Total U.S. VC**

Looking at the 2018 dual use venture funding by round reveals insights that will better shape innovation strategy. As Figure 4 shows, whether by intent or not, A and B Round funding is rather robust. However, the levels drop in the Late Stage, illustrating the need to shift focus.

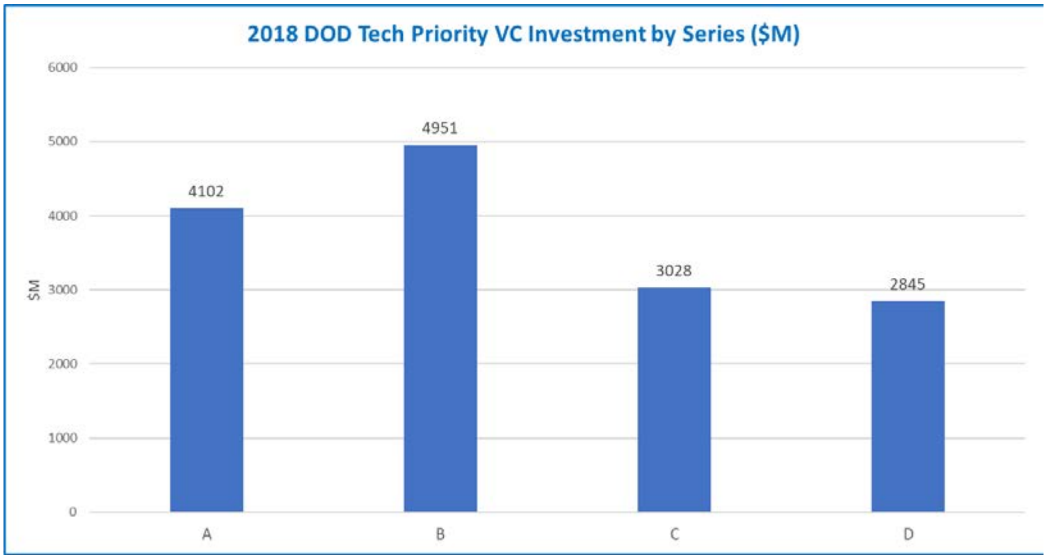


Figure 4. **2018 DoD Tech Priority VC Investment by Series**

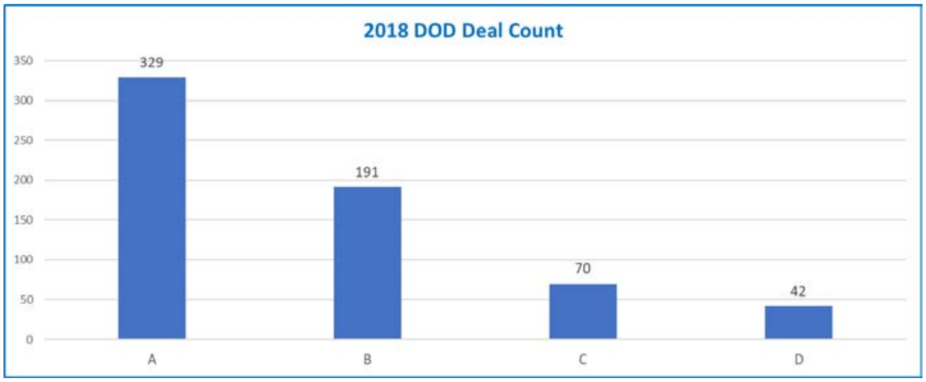


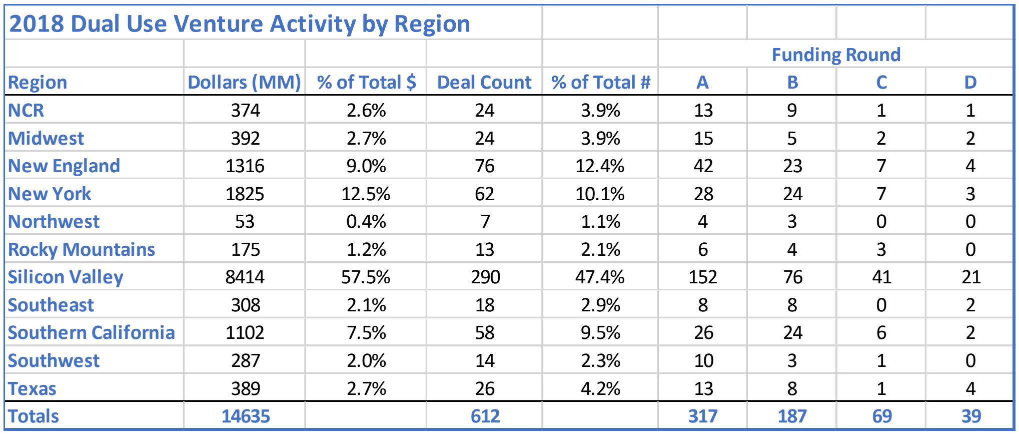
Figure 5. **2018 DoD Deal Count**

2018 Dual Use Venture Activity by Region

Table 1 shows 2018 dual use venture activity by region and funding stage. Table 2 compares DoD innovation unit budgets to venture activity by region.

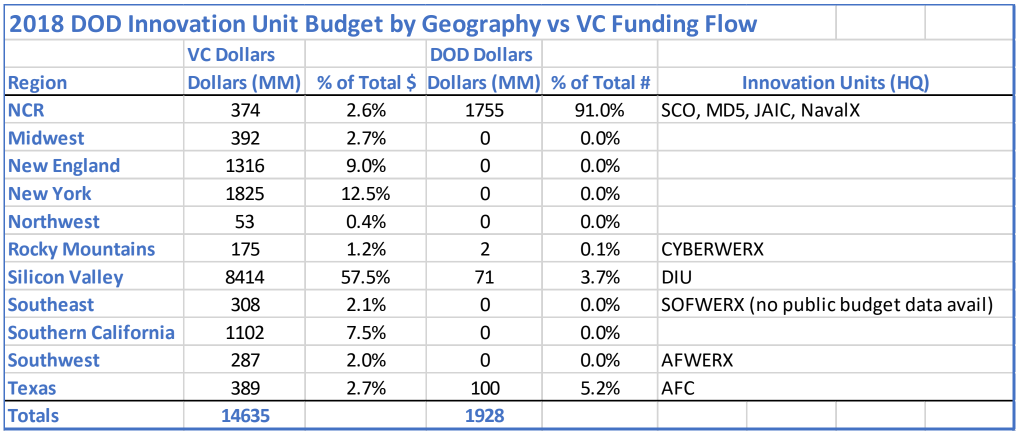
One immediate conclusion jumps off the page: Silicon Valley completely dwarfs all other regions. Similarly, from the second chart, DoD innovation is significantly over-indexed to the National Capital Region (NCR) and extremely under-indexed to Silicon Valley. SV had 57.5% of 2018 dual use venture flows. However, the DoD only allocates 3.7% of its VC-backed innovation engagement budget there, with just a single unit deployed there. The DIU needs a massive resource increase as the only unit based in Silicon Valley. The NCR gets 91% of DoD budgets with a mere 2.6% of venture funding. Lastly, the AFC's selection of Austin for its HQ implies other priorities for the unit than engagement with venture backed companies. Texas only saw 2.7% of venture funding in dual use categories last year.

Table 1. 2018 Dual Use Venture Activity



2018 Dual Use Venture Activity by Region								
					Funding Round			
Region	Dollars (MM)	% of Total $	Deal Count	% of Total #	A	B	C	D
NCR	374	2.6%	24	3.9%	13	9	1	1
Midwest	392	2.7%	24	3.9%	15	5	2	2
New England	1316	9.0%	76	12.4%	42	23	7	4
New York	1825	12.5%	62	10.1%	28	24	7	3
Northwest	53	0.4%	7	1.1%	4	3	0	0
Rocky Mountains	175	1.2%	13	2.1%	6	4	3	0
Silicon Valley	8414	57.5%	290	47.4%	152	76	41	21
Southeast	308	2.1%	18	2.9%	8	8	0	2
Southern California	1102	7.5%	58	9.5%	26	24	6	2
Southwest	287	2.0%	14	2.3%	10	3	1	0
Texas	389	2.7%	26	4.2%	13	8	1	4
Totals	14635		612		317	187	69	39

Table 2. DoD Innovation Unit Budget



2018 DOD Innovation Unit Budget by Geography vs VC Funding Flow					
	VC Dollars		DOD Dollars		
Region	Dollars (MM)	% of Total $	Dollars (MM)	% of Total #	Innovation Units (HQ)
NCR	374	2.6%	1755	91.0%	SCO, MD5, JAIC, NavalX
Midwest	392	2.7%	0	0.0%	
New England	1316	9.0%	0	0.0%	
New York	1825	12.5%	0	0.0%	
Northwest	53	0.4%	0	0.0%	
Rocky Mountains	175	1.2%	2	0.1%	CYBERWERX
Silicon Valley	8414	57.5%	71	3.7%	DIU
Southeast	308	2.1%	0	0.0%	SOFWERX (no public budget data avail)
Southern California	1102	7.5%	0	0.0%	
Southwest	287	2.0%	0	0.0%	AFWERX
Texas	389	2.7%	100	5.2%	AFC
Totals	14635		1928		

All the data relating to venture funding in this paper, unless otherwise noted, is targeted at DDRE Griffin's 10 tech priorities for the DoD (Acquisition in the Digital Age [AiDA]—MITRE, n.d.).

Case Study: AI/ML

Artificial Intelligence/Machine Learning (AI/ML) stands as a compelling case study candidate for a variety of reasons. Highest among those is the fact that the White House (Trump, 2019) and the DoD (2019) just released strategy papers, the Joint Artificial Intelligence Center was recently launched under General Shanahan (Cullum, 2018), and the category represents a huge amount of dual use venture funding (65.6% in 2018). This case study illustrates how the analysis of venture funding by stage and source better informs DoD innovation strategy.

AI/ML funding is showing immense growth and taking a steadily increasing share of venture funding (see Figure 6), all good news for the DoD's AI ambitions. Venture investors have poured billions into AI/ML deals. The total from 2014 to 2018 according to Pitchbook stands at $22.6 billion. This number alone clearly shows the DoD should focus on partnering with existing dual use AI start-ups rather than creating new ones.

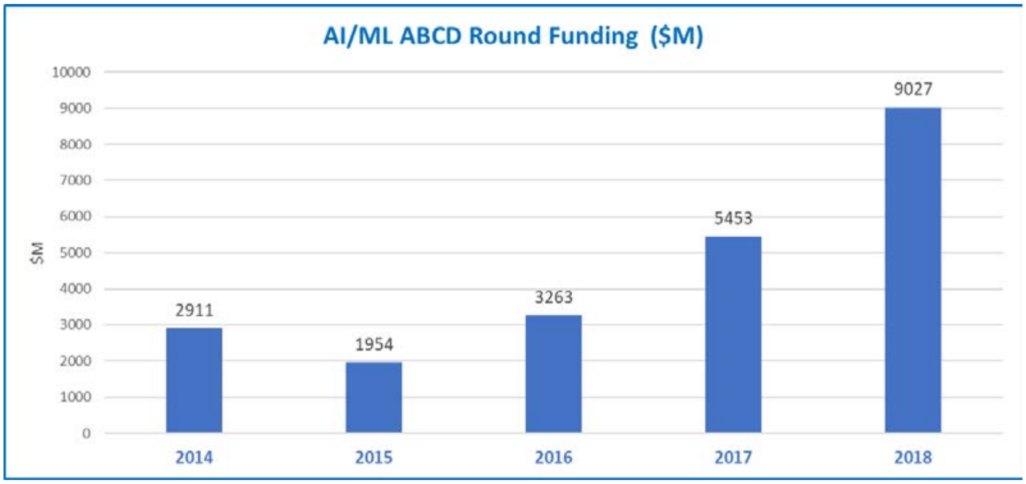


Figure 6. AI/ML ABCD Round Funding

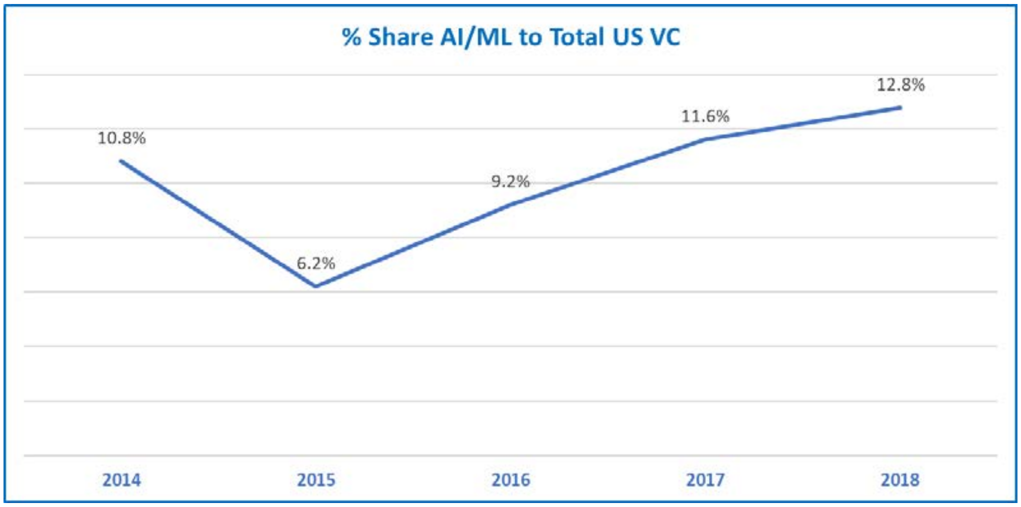


Figure 7. **Percentage Share of AI/ML to Total U.S. VC**

However, a closer look at 2018 funding data shows a more nuanced story. While A and B Round funding remains healthy, Late Stage funding drops dramatically (see Figure 8). AI technology has yet to find revenue-rich markets, making Late Stage funding difficult. This represents an opportunity for the DoD to aggressively compete for the attention of A and B Round companies with large procurements without onerous compliance and accounting requirements, thereby potentially attracting Late Stage funding that is currently sitting on the sidelines.

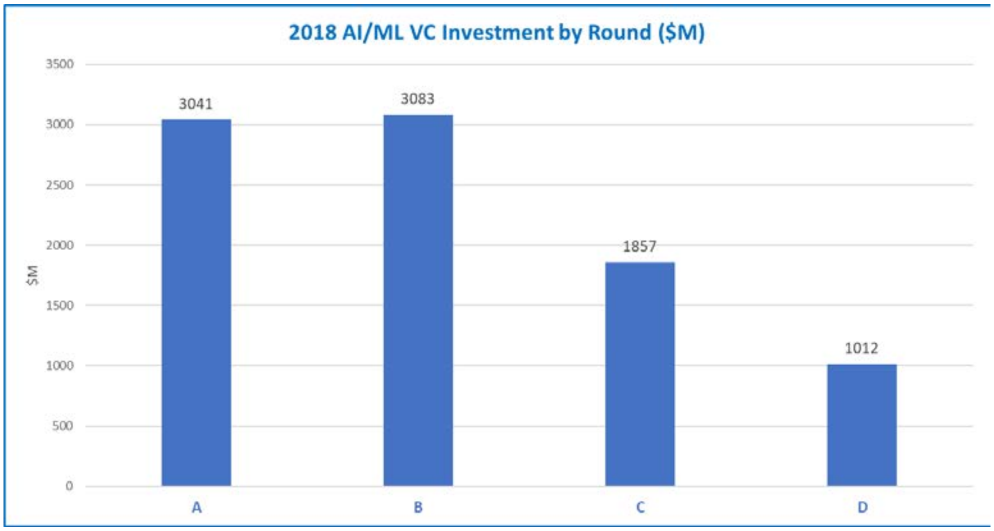


Figure 8. **AI/ML VC Investment by Round**

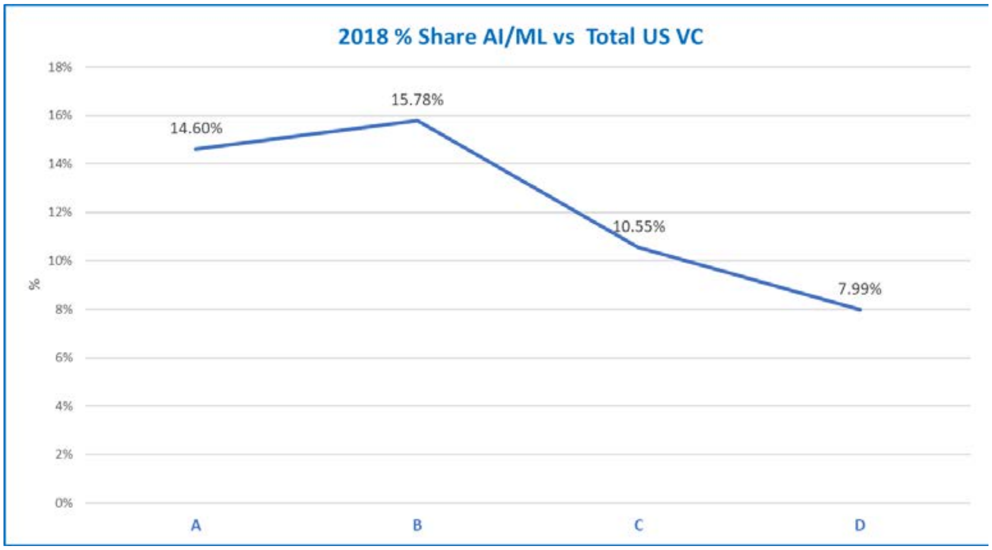


Figure 9. **Percentage Share AI/ML vs. Total U.S. VC**

Those efforts to woo capital and start-ups in AI should center around the West Coast. According to CB Insight's 4Q18 venture reports (PitchBook, 2019), the top five states for AI deals in the quarter were

- CA: 53 deals, $1.9 billion invested
- MA: 13 deals, $247 million invested
- NY: 10 deals, $110 million invested
- TX: 3 deals, $10 million invested
- WA: 3 deals, $9 million invested

Again, this illuminates Army Future Command's decision to HQ in Austin. Naturally, proximity to testing ranges and resources at Fort Hood supports that move, but the lack of AI/ML start-ups does not. The recent spate of NYC-based DoD AI/ML hackathons also don't make sense from a geographic analysis.

A Venture Capital Map of the National Security Innovation Base

Better policy and innovation partnerships would flow easier if the DoD side better understood the structure and process of the people (venture being relationship-driven) they are trying to partner with, especially considering that the DoD needs Silicon Valley more than Silicon Valley needs the DoD. The goal of this section, then, is to increase the effectiveness of DoD innovation efforts by decreasing the awkwardness of its efforts to attract innovation. Metaphorically, stop stepping on your dance partner's shoes by actually learning the dance.

Following is a highly simplistic model that captures the life stages of a venture backed dual use start-up as it progresses through the innovation ecosystem, describes the relevant issues for DoD support of that process at each stage, and recommends policies for improvement thereof. In the next section, the paper will then offer a basic framework for measuring the effectiveness of the DoD's efforts in stimulating greater output of dual use companies from this ecosystem.

Many of the terms and acronyms will be defined in the following section. However, a few definitions up front are necessary:

- Start-Up Stage—the general timeframe and lifecycle in which the start-up is currently operating. Innovation policy needs to fit each stage; one size does not fit all.
- VC Funding Round—the specific funding round that the start-up either most recently completed or is working to fund. These rounds somewhat fit the start-up stages, but not perfectly. The key is that as the start-ups move through their life stages, their funding round sources and milestones shift. Policy should fit appropriately.
- Sand Hill Road—the geographic location west of Stanford University in Palo Alto, CA, where the vast majority of the leading venture capital firms are located, especially those capable of writing large, late stage checks. The term "Sand Hill Road" is also often used as a metaphor for traditional venture funding.
- MVP—Minimum Viable Product, the goal of an early stage start-up, which is to go through multiple customer engagements as it defines its MVP, then build a business model. Many policy makers mistakenly confuse the order: MVP first, then detailed business model.
- DoD Innovation Units—DIU: Defense Innovation Unit; AFC: Army Futures Command; AFWERX: Air Force innovation outreach unit; SOFWERX: Special Operations Forces innovation, outreach unit; MD5: National Security Technology Accelerator; H4D: Hacking for Defense. This purposely excludes traditional DoD innovators such as DARPA, AFRL, NRO, etc.

DoD Innovation Outreach Ultimate Goal

In the interest of starting with the end in mind, the ultimate goal of DoD innovation efforts should first be defined. As referenced in the introduction, the obvious answer to that question is threefold from the perspective of a Silicon Valley venture investor: to motivate more founders to launch dual use start-ups, attract an increasing amount of private capital to fuel those start-ups' growth, and develop better policy to enable the services to deploy the technology from these companies. Or more simply put, the goal of DoD Innovation is to increase the number of "Dual Use Unicorns"[2] like Palantir, SpaceX, Cloudflare, Tanium, C3IOT, etc., by an order of magnitude.

While the DoD may not care about helping start-ups make unicorn status, only the larger Late Stage companies can handle the onerous requirements of full Federal Acquisition Requirements. In addition, the venture funders will require large exits at the Late Stage to continue finding dual use companies in the long term. Successful exits renew the innovation ecosystem. They are the key to driving the self-funding nature of the venture market. The proceeds of the exit go to the VCs who often re-invest them in earlier stage deals. As the number of successful exits grows, the amount of capital available in that ecosystem grows over time as well. For example, according to Crunchbase, a leading source of start-up financing data, the average successful startup raises $41 million in capital and exits for an average of $242.9 million (Lapowsky, n.d.). So, the DoD stands to benefit from a growing, self-funded source of new technology.

[2] A "unicorn" is Silicon Valley vernacular for a private (pre-IPO) venture backed company whose last financing round was conducting at a valuation exceeding $1 billion.

Creating Late Stage winners is easier said than done. In 2018, VCs funded 317 A Rounds but only 39 D Rounds. However, the DoD can boost the number of D Rounds if it properly aligns its current outreach units and budgets more effectively by stage, sector, and geography.

To do that, leadership needs to first understand the unique issues involved in supporting a start-up through its journey from Day 1 to Exit. It's generally understood in the Valley that the average time from start-up Day 1 to Exit is around seven years (Abdullah, 2018). Exact data on that number is difficult to measure with perfect accuracy because much of the data in the early stages is inconsistently self-reported. As discussed later, the data becomes much more reliable around the A Round.

Defining Foundational Venture Stage Concepts

Start-Up Lifecycle Stages: The lifecycle of a start-up proceeds in stages. These are generally referred to as Early, Mid, and Late Stage. Venture Capital firms often define their investment strategies by these stages. For example, Bessemer is known as a Mid Stage firm with emphasis on B Rounds, whereas Technology Crossover Ventures is very Late Stage focused, writing checks into five+ year old start-ups near their exits. The stage focus dictates what size of fund these VCs raise.

The average check size of an Early Stage Seed fund in 2018, according to Pitchbook, was $1.8 million. A venture fund normally targets 10–15 deals in its 7–10-year life. Thus, a Seed fund would need to raise around $20–50 million for the handful of partners to effectively deploy the fund in a timely manner.

Short Funding Stages Enforce Speed: Each stage usually holds one to three financing rounds. To move through these rounds, the start-up needs to achieve certain milestones. Funding rounds are usually spaced 12–18 months apart. Investors fund just enough cash in each round for the company to work towards its milestone, enabling the solicitation of the next funding round at a higher valuation. This structure drives the impressive speed in technology development which attracts the DoD—the start-up team either hits its milestone or goes "cash out."

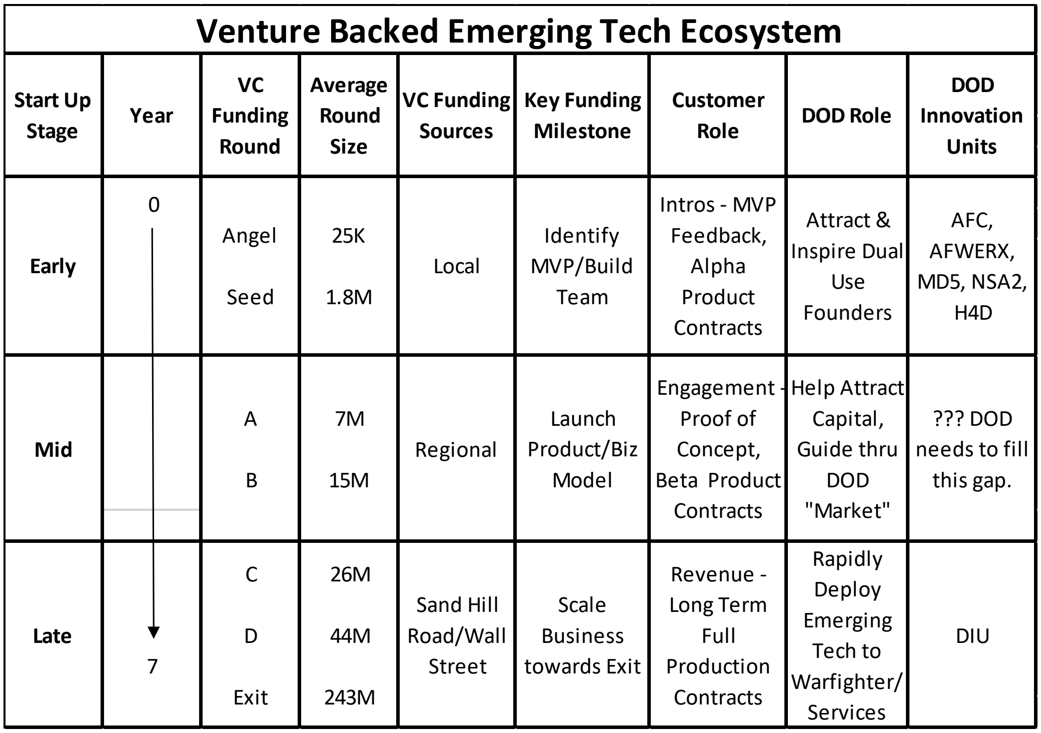
Founders' Equity Incentivizes Speed: The other driver of start-up speed is the incentive of the equity ownership. The founders stand to make a tremendous amount of money through their equity holdings if they get to a successful exit. Thus, they are willing to take extremely low cash compensation and run a very lean operation. This second feature of start-ups is also attractive to DoD innovation goals. Traditional DoD R&D development programs are often very slow and end up wasting billions, as was the case with the Army's Future Combat System program.

Key Funding Milestones: For a start-up to obtain its next funding round, it must first achieve the key milestone enabled by its current funding round. DoD innovation policy makers should a have rudimentary understanding to better align resources by stage.

The key milestone in each stage evolves as the company grows. In the Early Stage, according to the work of leading start-up theorist and Stanford professor Steve Blank, the company is searching for its Minimum Viable Product (MVP; Blank, 2013) while building out the team beyond the first founders (usually one to three, with more than five being relatively rare). In the Mid Stage, the company raises more money to build the MVP into a full featured product ready for general availability with a full-fledged business plan and revenue model. In the Late Stage, the company raises even more money, often upwards of $100 million or more, to scale business towards an exit by hiring a large sales force and launching a comprehensive marketing campaign with the goal of ensuring a profitable exit.

The DoD needs to meet start-ups at each of their life stages with the right combination of customer engagement and financial support that helps the companies move more effectively towards their next funding round, yet this assistance must also be supportive of the ultimate exit.

For instance, the start-up's board of directors will often reject early stage Non-Recurring Engineering (NRE) money from a DoD source if they don't see a pathway from that activity towards a full Program of Record opportunity. The NRE may seem nice in a vacuum, but investors at the next funding round will not "count" that revenue in their valuation if it's not indicative of a much larger market opportunity later (usually referred to as TAM or Total Addressable Market).



Venture Backed Emerging Tech Ecosystem

Start Up Stage	Year	VC Funding Round	Average Round Size	VC Funding Sources	Key Funding Milestone	Customer Role	DOD Role	DOD Innovation Units
Early	0	Angel Seed	25K 1.8M	Local	Identify MVP/Build Team	Intros - MVP Feedback, Alpha Product Contracts	Attract & Inspire Dual Use Founders	AFC, AFWERX, MD5, NSA2, H4D
Mid		A B	7M 15M	Regional	Launch Product/Biz Model	Engagement - Proof of Concept, Beta Product Contracts	Help Attract Capital, Guide thru DOD "Market"	??? DOD needs to fill this gap.
Late	7	C D Exit	26M 44M 243M	Sand Hill Road/Wall Street	Scale Business towards Exit	Revenue - Long Term Full Production Contracts	Rapidly Deploy Emerging Tech to Warfighter/ Services	DIU

Figure 10. **Venture Backed Emerging Tech Ecosystem**

Early Stage—Funding Stages and Sources

The Angel and Seed rounds constitute what is called the Early Stage. Note that Early Stage funding data is less reliable than later stage data due to the self-reporting issue. Therefore, this paper is only analyzing A Rounds and later. The Mid and Late Stage sections will start with a review of 2014–2018 dual use funding trends.

Angel Round—On Day 1, when a start-up is first formed through the signing of Articles of Incorporation, it finds financing in one of three ways: either by "bootstrapping" with the help of friends and family, or by securing launch funding from an Angel Investor. Bootstrapping is when the founders use their own money to finance operations. An Angel Investor is a professional venture investor who specializes in investing in a start-up's first round by using outside capital. Angels are almost exclusively high-net-worth individuals, though they often group together in networks. The function of the Angel is to partner with the founders to move them from the "cocktail napkin idea" stage to where they can receive their first full VC funding round from a traditional Venture Capital Limited Partnership (or the equivalent thereof, like a corporate entity making an early stage minority investment—the nuances are not relevant to the purposes of this paper). Both sources of funding described in this paragraph are usually lumped together under the name Angel Round for convenience.

Seed Round—While usually still pre-revenue, here the start-up usually accepts its first capital investment from a professional venture firm. The importance is that the company has somewhat graduated from the "hobbyist" start-up phase to being serious enough to attract investor attention.

Most major cities have an adequate number of Angel and Seed investors that a founder can get all their financing done locally, as shown by the CB Insights chart in Figure 11. Thus, the DoD does not need a national level function working to organize and attract early stage funding for dual use start-ups. The local innovation units can address that issue organically in their own local venture networks.

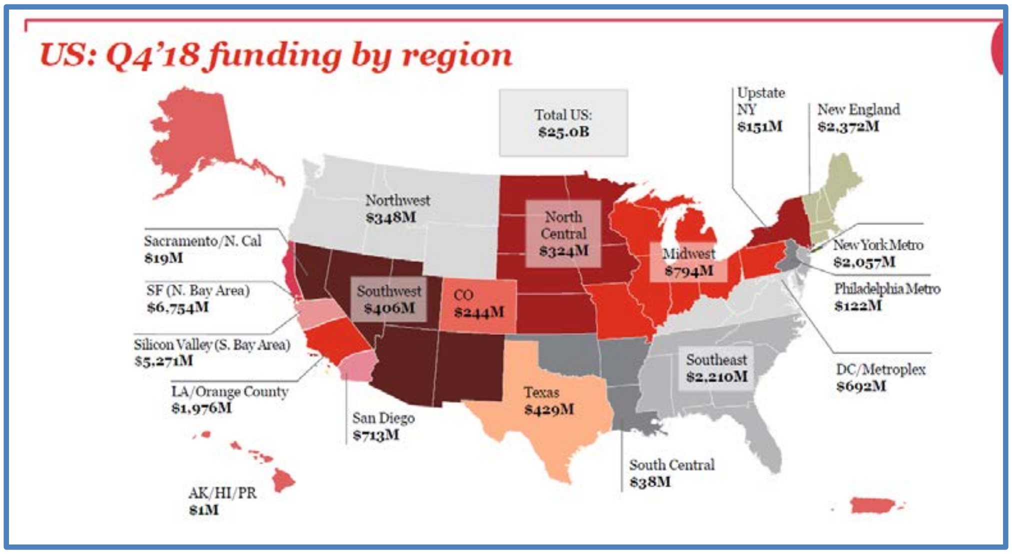


Figure 11. **Q4'18 Funding by Region**

Early Stage—DoD Innovation Units

The DoD is heavily resourced in its efforts at the Early Stage. A couple of units stand out as notable:

- Hacking4Defense (H4D): According to the H4D website, "Hacking for Defense™ is a university-sponsored class that allows students to develop a deep understanding of the problems and needs of government sponsors in the DOD and IC." The DoD funds H4D, with classes conducted at approximately 20 schools in the fall of 2018 (Johnston, 2018). H4D is an extremely well thought out program (if one endorses the Lean Start Up methodology) for launching dual use founders on Day 1 through Day 90 when the three-month course ends. The formal timeline begs the question of what happens next when a start-up graduates … enter MD5 …
- MD5: Otherwise known as the National Security Technology Accelerator (and rumored around Silicon Valley to be up for a new name and reporting structure

change), the mission of MD5 is to “create new communities of innovators that solve national security problems.” MD5 is well positioned to provide the “Sherpa” function described previously, especially for H4D graduates who need support in their early stage dual use mission from Day 91 through their Seed Round. MD5 is well positioned for three reasons:

1. DoD-Wide: MD5 represents the entire DoD, whereas other early stage outreach units like AFWERX are beholden to a specific service.
2. National Geographic Focus: provides the comprehensive nation-wide network necessary to harness every single state (i.e., and more importantly, every Congressional district)
3. University Focused: a natural hub from which the surrounding innovation ecosystem can be effectively organized, whereas other early stage units lack a consistent geographic home in each geography which leads to inconsistent deployments of resources across regions

- AFC: The Army Futures Command is a vitally important evolution of the DoD innovation outreach strategy. As referenced in the introduction, none of this emerging technology partnering rhetoric matters if it doesn’t end up deployed across the services in the hands of the warfighter. Additionally, the AFC has the largest budget of any services innovation unit at $100 million, a four-star commander, and responsibility for the Army’s entire $30+ billion modernization budget (Freedberg, 2018). However, at least for now, its geographic choice of Austin positions it as an Early Stage player. The southern region, including Texas, Oklahoma, Arkansas, and Louisiana, only account for 6.6% of all venture deals and a meager 2.4% of all venture funding in the United States in 2018, according to the National Venture Capital Association (PitchBook & National Venture Capital Association, 2018).

Early Stage—DoD Goals

In the simple three phase DoD innovation outreach framework described earlier, here is where DoD innovation outreach efforts should be focused on motivating founders to start a company, and/or direct their start-up towards dual use applications. The earlier a start-up embraces the DoD as a customer or security as a market, the more likely it is to develop technologies of interest. This could be thought of as the “battle for hearts and minds in the garages and dorm rooms,” and thus, the Early Stage DoD outreach efforts should be calibrated to this goal.

Mapping the Local Start-Up Ecosystem: In addition to founder-oriented outreach, these Early Stage DoD units need to map out their local/regional innovation. They need to identify all the resources in their assigned region that could support their cause and potentially benefit dual use start-up founders in their company’s first years. Of utmost importance are the Angel Investors described previously and the Angel Networks. All the existing university-based incubators, entrepreneurs clubs, innovation leadership, etc., would also need to be mapped out along with supportive military influence groups such as San Diego’s Military Advisory Council. These are relationship-based networks such that a traditional military rotational assignment model won’t do—another reason that MD5 should serve as the permanent civilian “connective tissue” of the Early Stage.

There a few key efforts here that must be effectively conducted, and somewhat in order:

1. Founding of the dual use start-up—essentially getting from “cocktail napkin” to Articles of Incorporation (Day 1) with Founder’s Equity divvied up among the small number of founders.
2. Incubation (Day 2 through Seed Funding)—Many innovation locales have existing incubators. The DoD should partner there as much as possible. If adequate and effective local incubators don’t exist to serve dual use startups, DoD innovation outreach units may need to start their own. Incubation is where the start-up founders hire employee #1 while beginning the search for their MVP.
3. Customer Intros—The early stage start-up needs as many customer introductions as possible to get input on their MVP. Here the DoD outreach folks can help by providing these introductions to the local DoD units and related agencies. This is probably the single most important function of the DoD outreach units at the early level—to break down barriers between civilian start-ups and local defense entities. Merely getting on base to engage with local military leaders is nearly impossible for civilian founders.
4. Modest Funding—Early Stage start-ups can benefit from small amounts of DoD non-dilutive capital in the form of grants and non-recurring engineering funding. These amounts should probably mirror the practice of commercially-oriented incubators, who often give $50,000–150,000 in funding in exchange for small pieces of equity. The funding helps the start-up get through its first 90–365 days. The DoD money should come with no strings attached and even perhaps no deliverables. The funding is to help the start-up engage with potential DoD customers as the founders search for their MVP. Prototyping comes later and marks the beginning of a multi-year journey from OTA style “no-strings” attached defense contracts towards full rate production Program of Record contracts with full FAR12/15 accounting requirements.

Mid Stage—Funding Trends

As Figures 12–13 show, funding in the Mid Stages appears healthy and growing. The rough total of $9 billion in Mid Stage funding ($4.1 billion A and $4.95 billion B) is encouraging considering how little the DoD has invested in stimulating this funding. As shown later, FY2019 budgets for innovation units focused explicitly on venture backed companies totals less than $2 billion and is arguably closer to a few hundred million depending on how one views the Strategic Capabilities Office (SCO).

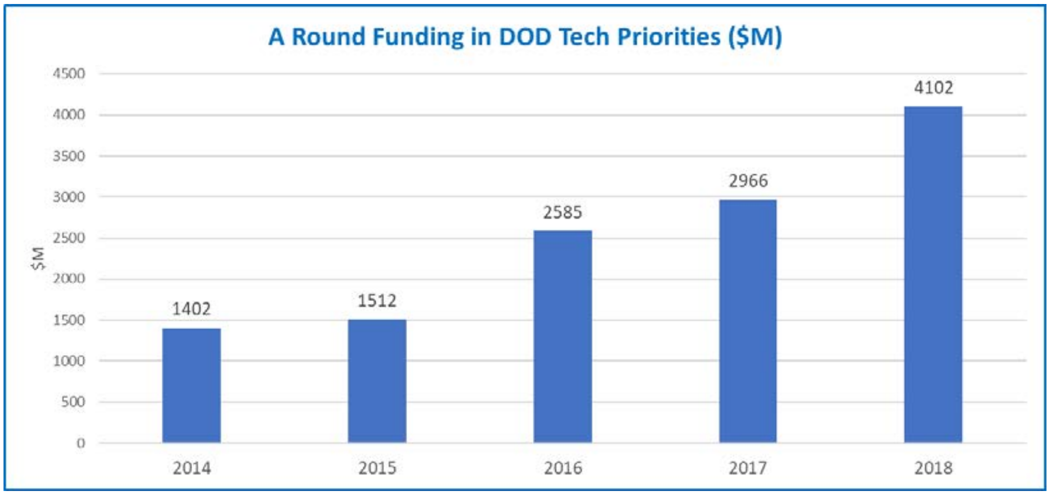


Figure 12. **. A Round Funding in DoD Tech Priorities**

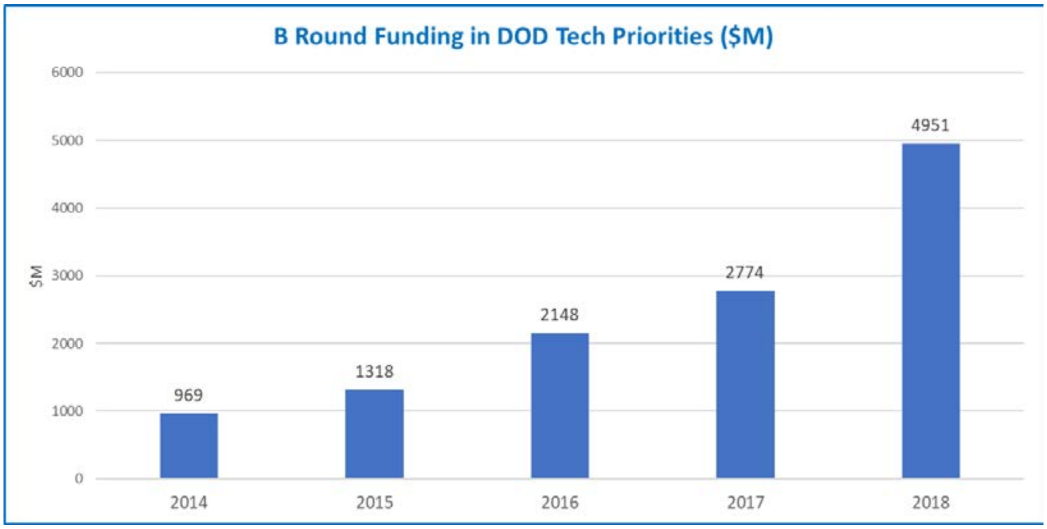


Figure 13. **B Round Funding in DoD Tech Priorities**

Mid Stage—Funding Stages and Sources

Start-ups crossing the line from the Seed to the A Funding Round also cross the "magical" line from Early Stage to Mid Stage. They are taken much more seriously by professional venture investors. What's important for DoD innovation policy makers is that the sources of funding for Mid Stage dual use begin to narrow and are concentrated more geographically.

A and B Round checks are much larger, averaging $7 million and $15 million in 2018 according to PitchBook. Funding sources capable of writing checks to fit these round sizes are not as readily found in all 50 states. Potential funding partners move from being available locally to mostly being found regionally in the largest cities with the more robust innovation ecosystems. Silicon Valley and the West Coast become more important partners for the DoD and dual use starts ups in the Mid and Late Stages. According to PitchBook's 4Q18 Venture Monitor, the West Coast region funded 61.7% of all VC funding in 2018 (PitchBook, 2019).

This is good news in one sense for the DoD, as it can start focusing its resources geographically towards these funding centers, as the founders will naturally begin building relationships into the networks that can support their next funding rounds.

Mid Stage—DoD Units

There aren't any.

That is a bit of an overstatement, as almost all the DoD innovation outreach units conduct activities that touch the Mid Stage. However, none of them are specifically aimed at this stage with the correct regional focus. The non-defense equivalent here would be an organization like Galvanize with a network of co-location Accelerators deployed in key innovation regional hubs like Denver and San Francisco.

A later section in this paper will survey the majority of the well-known DoD innovation units, where this gap will be more readily addressed. Also, the role of the DIU comes up here. It is based primarily in Silicon Valley with tiny satellite offices in Austin and Boston. So, it would seem natural that it targets the A/B Rounds; which it does. However, as this paper will argue later, the DIU is uniquely positioned to support the DoD in the Late Stage where the checks, stakes, and potential warfighter impact are much greater.

Mid Stage—DoD Goals

The role of DoD innovation units changes as they move into the Mid Stage. Happy hours, free T-shirts, and Sherpa services are no longer as useful to dual use start-ups here. Their Key Funding Milestones require more substantial help if they are going to continue with a defense focus. Beyond customer introductions, they need revenue from early customers not so much to fund their business models, but rather to validate their Minimum Viable Product.

DoD innovation interactions at the Mid Stage, then, should focus on finding DoD customers with priority problems and an agile contracting capability (Other Transaction Authorities being top of that list), and matching them with the most promising dual use start-ups. This is easier said than done. The Federal Acquisition Regulation makes this sort of "customer interfacing" activity extremely difficult for the outreach unit attempting to act as the intermediary. However, the laws of venture funding are as firm as gravity, and they don't care about the need to first issue a Broad Area Announcement and then wait 90 days before undertaking vendor meetings. Those 90 days put the start-up one quarter closer to death (otherwise known as "cash out").

To address the issue raised in the preceding paragraph, the DoD has deployed all sorts of innovation funding experiments, dedicated funds, and related activities. However, no central directory thereof exists. The DoD innovation outreach units need to help solve this discovery problem in their regions. Just as they mapped out the Angel Networks in the Early Stages to better make funding introductions for their incubating dual use start-ups, they must also map out the DoD agile funding ecosystem.

They similarly need to map out the A and B Round funding sources. This should include determining which VCs have accepted Chinese LPs and discouraging dual use founders from taking their money.

Finally, Mid Stage companies are mature enough to take the "on ramp" to a five-year journey from OTA prototyping contracts with minimal paperwork towards PEO full rate/full paperwork prime contracts. The DoD should work to more officially define this "on ramp" approach so that the paperwork requirements match the life stage of the start-up. For instance, an A Round company may be able to support some very modest form of cost reporting but not a full-blown Defense Contracting Acquisition Agency audit. To that point, professional venture investors rarely ask for fully audited financial statements until the company is nearing its exit, usually with $100+ million in revenue. They would rather the management team focus on growth rather than perfect accounting. The primary financial focus until the exit is on revenue growth, cash burn rate, and cash balance.

Late Stage—Funding Trends

Funding for C Round companies shows nice growth progress, though the level in 2018 is down roughly $1 billion from the $4+ billion in the A and B Rounds (see Figure 14). D Round funding shows a more volatile pattern with strength in the last two years (see Figure 15).

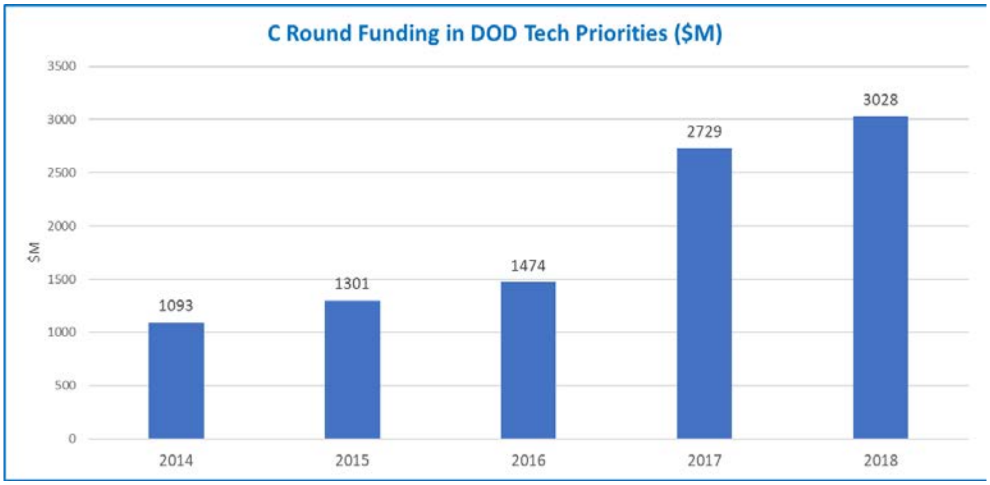


Figure 14. **C Round Funding in DoD Tech Priorities**

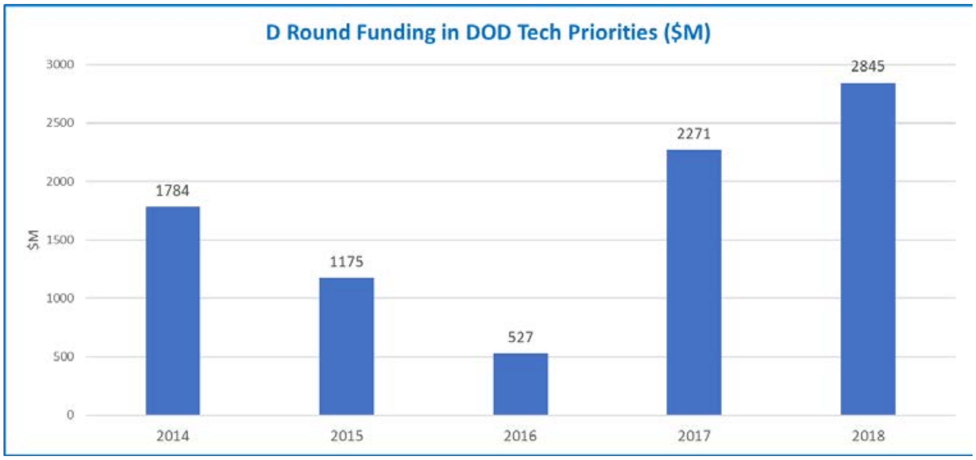


Figure 15. **D Round Funding in DoD Tech Priorities**

Late Stage—Funding Stages and Sources

Late Stage funding sources become very concentrated. With a few rare exceptions (large family offices, corporates, and sovereign wealth funds), most of the late round equity financing either comes from Sand Hill Road or Wall Street. According to the PitchBook data, 16 of the top 20 most active Late Stage investors in 2018 were based in Silicon Valley.

The average check sizes (total) for C and D Rounds were $26 million and $44 million in 2018. The days of the founder asking his or her parents for some funding are long behind. As pointed out earlier, the West Coast (mostly Silicon Valley) provided 61.7% of 2018 venture financing. However, the region only financed 39.5% of all deals, which speaks to the much larger check sizes.

Late Stage—DoD Units

There should only be one unit focused on the late stage. The DIU is uniquely positioned by geography to manage the Late Stage VC relationships on behalf of the DoD. Venture investing is a relationship-based business. If the DoD wants to attract large checks for its dual use start-up partners, it needs to establish good relationships with those check writers, and those large check writers, like TCV, Andreesen Horowitz, New Enterprise Associates, etc. have more money than time. They and their peers are not interested in meeting every single DoD innovation outreach unit under the sun—AFWERX, CYBERWERX, SOFWERX, DIU, MD5, NavalX, AFC, SCO, REF, and especially those that use a traditional uniformed rotational assignment process.

Second, the PEOs need one authoritative emerging technology partner upon which they can base their long-term acquisition planning. As the PEOs can't integrate dual use start-ups until the Late Stage due to the overhead requirement, that authoritative partner probably should be the same one coordinating the Late Stage VC relationships.

Late Stage—DoD Goals

The Late Stage is where the DoD can finally achieve its ultimate goal of rapidly deploying new emerging technology in the hands of the warfighter at scale. That sounds an awful lot like an official Program of Record.

The early PEO partnerships discussed previously are critical so that by the time the start-ups have scaled enough to afford DoD overhead, the PEOs had their requisite five years lead time to plan to incorporate the start-ups' new technology in their acquisition plans.

Without the PEOs and their Programs of Record, the start-ups lack a big enough customer representing a sufficiently large Total Addressable Market to support an exit and justify their choice of the DoD as a target customer. Thus, the need for an exit drives start-up strategy at every stage. No exit; no VC funding.

Of course, the start-ups can always partner with Traditional Defense Contractors (Primes) and System Integrators (SIs), which they often do and should. However, these partnerships also take extensive time to materialize (and monetize), just as a DoD prime contract would, and the enhanced overhead requirements are still material, even in a sub-contracting role.

Conclusion

The early returns as measured in the dual use funding data described in this paper merit the strong support of National Security Leadership. With all due respect, the opposition to modest funding levels for organizations such as the DIU must stop. The primes and system integrators should instruct their government relations teams to stop opposing these seedling efforts and instead partner with them. Large defense contractors would be better served to fear Amazon's move into their market rather than the DIU. The latter wants to help them; the former wants to dominate them in the digital arms race.

Again, to make the point, China raised more money in one financing round from western investors for its leading AI company than Congress is willing to commit to the entirety of the DoD innovation units aimed at VC backed companies. Therefore, the early successes described in this paper should not cloud the fact that there is much work still to be done in winning the Digital Arms Race.

To complete the work of supporting the NSIB:

- Congress should fully fund from the appropriations side all the innovation efforts supported from the authorizer side.
- The DoD should deconflict and better coordinate all its innovation units at the OSD level.
- The Services should compel their PEOs to collaborate with the innovation units.
- The Primes should all launch their own venture funds, partner with dual use funds, and make strategically meaningful minority investments into Late Stage dual use companies. They should also increase commercial technology leadership on their boards of directors.
- The System Integrators should facilitate the introduction of emerging technology companies to their customers in partnership rather than continuing to propose building their own (often antiquated upon delivery) custom technology solutions, particularly in software.

True success, finally, will be achieved when venture backed dual use start-up IPOs are commonplace. Only then will the dual-use ecosystem become self-sustaining and the full power of U.S. free markets be brought to bear on this new age of the Great Power Competition.

References

Abdullah, S. (2018, November 25). How long does it take a startup to exit? *Crunchbase*. Retrieved from https://about.crunchbase.com/blog/startup-exit/

Acquisition in the Digital Age (AiDA)—MITRE. (n.d.) USD(R&E) top 10 technology focus areas. Retrieved from https://aida.mitre.org/top-10-technology-areas/

Baig, M. A. (2019, March 10). Gerasimov doctrine and hybrid war. *Daily Times*. Retrieved from https://dailytimes.com.pk/295075/gerasimov-doctrine-and-modern-hybrid-war/

Blank, S. (2013, May). Why the lean start-up changes everything. *Harvard Business Review.* Retrieved from https://hbr.org/2013/05/why-the-lean-start-up-changes-everything

Cullum, J. (2018, December 14). DoD CIO: Joint artificial intelligence center ‘up and running.’ *Homeland Security Today*. Retrieved from https://www.hstoday.us/subject-matter-areas/cybersecurity/dod-cio-joint-artificial-intelligence-center-up-and-running/

DoD. (2018). *Summary of the 2018 national defense strategy of the United States of America*. Retrieved from https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

DoD (2019). *Summary of the 2018 Department of Defense artificial intelligence strategy: Harnessing AI to advance our security and prosperity*. Retrieved from https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

Elias, J. (2018, September 24). Former Symantec CEO named to head Defense Department’s Silicon Valley unit. *Silicon Valley Business Journal*. Retrieved from https://www.bizjournals.com/sanjose/news/2018/09/24/dod-diu-silicon-valley-unit-michael-brown-symantec.html

Freedberg, S. (2018, August 29). Army Futures Command: $100M, 500 staff, and access to top leaders. *Breaking Defense*. Retrieved from https://breakingdefense.com/2018/08/army-futures-command-100m-500-staff-access-to-top-leaders/

Johnston, R. (2018, September 21). ‘Hacking for defense’ course to be taught in 20 universities this year. *EdScoop*. Retrieved from https://edscoop.com/hacking-for-defense-course-to-be-taught-in-20-universities-this-year/

Lapowsky, I. (n.d.). $243 million: Crunchbase’s very rosy picture of the average startup exit. *Inc*. Retrieved from https://www.inc.com/issie-lapowsky/average-successful-startup-exit.html

Mattis, J. (2018, December 1). Remarks by Secretary Mattis on national defense strategy [Transcript]. Retrieved from https://dod.defense.gov/News/Transcripts/Transcript-View/Article/1702965/remarks-by-secretary-mattis-on-national-defense-strategy/

PitchBook. (2019, January 9). 4Q 2018 PitchBook-NCVA venture monitor. (2019, January 9). Retrieved from https://pitchbook.com/news/reports/4q-2018-pitchbook-nvca-venture-monitor

PitchBook & National Venture Capital Association (n.d.). Venture monitor: 4Q 2018. Retrieved from https://nvca.org/research/venture-monitor/

Sanger, D. E., Barnes, J. E., Zhong, M., & Santora, R. (2019, January 27). U.S. scrambles to outrun China in new arms race. *The New York Times*.

Trump, D. (2019, February 11). Executive order on maintaining American leadership in artificial intelligence. Retrieved from https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/

Williams, L. (2018, February 12). DIUx gets a big boost in FY19 budget. *FCW.* Retrieved from https://fcw.com/articles/2018/02/12/budget-williams-dod.aspx

Panel 7. Using Technology to Innovative Defense Acquisition

Wednesday, May 8, 2019	
12:45 p.m. – 2:00 p.m.	**Chair: Major General Kirk Vollmecke, USA,** Program Executive Officer for Intelligence, Electronic Warfare & Sensors ***Smart Contracts in the Federal Government—Leveraging Blockchain Technology to Revolutionize Acquisition*** Michael Arendt, Patrick Staresina, Kenyon Doyle, and Dave Bryson, The MITRE Corporation ***Automatic Generation of Contractual Requirements From MBSE Artifacts*** Alejandro Salado and Paul Wach, Virginia Tech ***Computing Without Revealing: A Cryptographic Approach to eProcurement*** Siva Chaduvula, Jitesh Panchal, Ashish Chaudhari, and Mikhail Atallah, Purdue University

Major General Kirk Vollmecke, USA—Major General Vollmecke became the Program Executive Officer for Intelligence, Electronic Warfare, and Sensors at Aberdeen Proving Ground, MD in April 2016. In this position he is responsible for the development, acquisition, fielding, and life cycle support of the Army's portfolio of intelligence, electronic warfare, cyber, biometrics and target acquisition programs. These capabilities provide the Soldier with the ability to detect, recognize, and identify targets, as well as to collect, tag and mine intelligence which can be integrated into the tactical network to support force protection, maneuver, persistent surveillance, and provide a more detailed understanding of the battlefield.

MG Vollmecke was commissioned as a Second Lieutenant in May 1984 through ROTC as a distinguished military graduate of the Centre College of Kentucky, where he earned a Bachelor of Arts Degree in Economics and Management. He also graduated from the Naval Postgraduate School in 1992 where he earned a Master of Science Degree in Management with a concentration in Acquisition and Procurement Management. He is a 1999 graduate of the U.S. Army Command and General Staff and a graduate of the U.S. Army War College in 2004. MG Vollmecke is Acquisition Level III certified in Program and Contract Management.

Prior to his current position, MG Vollmecke served as the Deputy Program Executive Officer for Intelligence, Electronic Warfare and Sensors at Aberdeen Proving Ground, MD. He has also served as the Deputy Commanding General for the Combined Security Transition Command-Afghanistan (CSTC-A) overseeing the security assistance program for the Afghan National Defense Security Forces in support of OPERATIONS ENDURING FREEDOM and FREEDOM'S SENTINEL. His acquisition assignments include the Deputy for Acquisition and Systems Management, Office of the Assistant Secretary of the Army (Acquisition, Logistic and Technology), Washington DC, in which he provided program management oversight of Army acquisition programs. Prior to that assignment, MG Vollmecke was the Commanding General of the Mission and Installation Contracting Command (MICC), Fort Sam Houston, Texas which provided Army commands, installations and activities contracting solutions and oversight across CONUS. Before that, he served as the Deputy to the Deputy Assistant Secretary of the Army for Procurement to ASA(ALT). He also served on the Joint

Staff as the J-8 Chief, Capabilities and Acquisition Division, and before his tour on the Joint Staff in 2007; he was the Commander, Defense Contract Management Agency Iraq/Afghanistan supporting OPERATION IRAQI FREEDOM.

Other acquisition assignments include Headquarters Department of the Army Systems Coordinator for the Future Combat Systems (Brigade Combat Team) program, Executive Officer to the Assistant Secretary of the Army(AL&T); Commander, DCMA Boeing Philadelphia; Program Analyst for the Deputy Chief of Staff of the Army for Programs, Program Analysis and Evaluation (PA&E) Directorate; Assistant Product Manager M2/M3 for the Bradley Fighting Vehicle Systems project office; Contingency Contracting Officer assigned to the U.S. Army Forces Central Command-Saudi Arabia under OPERATION DESERT FALCON; and as a Weapon System Contracting Officer assigned to the Army Materiel Command's Communications-Electronics Command(CECOM), which included a deployment to Honduras, Joint Task Force Bravo. Prior to joining the Army's Acquisition Corps in 1991, he served in a variety of mechanized and light infantry battalion staff and company command positions.

Smart Contracts in the Federal Government—Leveraging Blockchain Technology to Revolutionize Acquisition

Michael Arendt—PhD, is a subject matter expert in innovative acquisition and contracting strategies across the Federal Government. Over the past 12 years, he has authored and co-authored numerous studies and reports including The *MITRE Innovative Contracting Implementation Framework*, *The MITRE Challenge-Based Acquisition Handbook*, *From Incentive Prize and Challenge Competitions to Procurement*, and *Pushing the Acquisition Innovation Envelope at the Office of Naval Research*. Arendt was a public-sector strategy and innovation consultant with IBM and a member of the research faculty at the University of Maryland's Center for Public Policy and Private Enterprise. He holds a PhD in Policy Studies from the University of Maryland, College Park.

Dave Bryson—is a lead engineer for the MITRE corporation with more than 20 years of experience designing and building software. In his current role as MITRE's blockchain technology lead, he performs research in applying the technology to the enterprise space and contributes to several leading open-source blockchain projects.

Kenyon Doyle—has more than 15 years of program management experience by serving in the United States Air Force, Federal Civilian workforce, and currently works in industry for The MITRE Corporation. Doyle has managed and supported defense acquisition programs covering aspects of the acquisition process, including research and development, integrating engineering, developmental and operational test, deployment, configuration management, production, manufacturing, and logistics support. Doyle has a BS in business administration from The Citadel and an MSA in general administration from Central Michigan University.

Patrick Staresina, COL, USA (Ret.)—is a retired member of the Army National Guard with more than 20 years of contracting officer experience, with the pinnacle of his Federal career serving as the Director of Contracting at the National Guard Bureau. Staresina continues to provide acquisition support the Federal Government through his service as an Acquisition Principal for multiple federally funded research and development centers (FFRDCs) managed by the MITRE Corporation.

Abstract

Across the government, the process of creating and enforcing contracts has not changed much in the past several decades. To this day, most government contracts require paperwork that must be routed across multiple parties, with physical signatures attested to by key personnel, and further rely on third parties such as private contractors or other government organizations for enforcement and storage. This results in a slow, opaque process that lacks transparency, efficiency, and auditability. Despite this reality, major advancements in blockchain technology in recent years have opened a new door to greatly improving the traditional government contracting process via the use of blockchain enabled, smart contracts.

Smart contracts have the potential to simplify many types of agreements (such as Government-Wide Acquisition Contracts and General Services Administration Schedules, among others) without the need for tedious paperwork and third parties. They can objectify contracts and policies while also storing the provenance of the information on a globally decentralized database. This research paper discusses how blockchain technology, coupled with smart contracts, can provide a next generation approach to automate and radically reduce acquisition lead time, improve contract performance, and sustainably decrease transaction costs.

Introduction

When most people think of blockchain, they immediately think of cryptocurrency and Bitcoin. For some, hearing these terms stimulates a cynical eyeroll as one recalls the last great, overhyped technological innovation whose promise far outweighed its practical, real-world benefits. While there are certainly some corners of the blockchain and cryptocurrency universe that will inevitably fail, there are many others that will meet and widely exceed promised expectations. Blockchain-based smart contracts are one of these innovations that has the potential to revolutionize the world as we know it.

This research paper provides a window into how blockchain-based smart contract technology can be leveraged across the federal, state, and local government to improve acquisition and procurement. Acquisition and procurement can be simply defined as the purchasing of goods and services. Both public and private sector entities acquire and procure a wide variety of things ranging from construction services to office furniture, from software licenses to printer paper, from IT consulting services to cloud-based technologies which serve as the backbone for day-to-day operations.

In the case of the government, whether it be federal, state or local, the process to acquire these goods and services tends to be complex. Irrespective of the level of government and department or agency doing the buying, a process exists for the express purpose of executing these transactions. Many involve a slew of requirements paperwork, reviews and approvals, bids and proposals, contract awards, administration, oversight of contract terms and conditions, inspection and acceptance criteria for delivery, and finally at some point taxpayer funds can be disbursed for payment. The resulting process can seem archaic for those in the government who practice it and twilight-zone-like for those in industry who are used to getting things done nearly on-demand. This is not to say that advancements have not been made in streamlining contracting processes, reducing acquisition lead-time, and making payment disbursements to vendors more efficient. But considerable opportunities for improvement remain to bridge the gap between government operations and commercial benchmarks for operating efficiency. Moreover, when examined today within the context of what is truly possible while employing a revolutionary technology like blockchain-enabled smart contracts, the promise for improvement may in fact be exponential. Numerous opportunities exist across a wide range of acquisition and procurement types to turn months into days or weeks to complete the very same transactions that currently drain the hope out of those caught in the middle of the process.

This research paper introduces blockchain technology; provides an overview of the status quo which may be colloquially referred to as “dumb contracts”; offers an introduction to blockchain-based smart contracts along with their benefits as well as drawbacks; describes a prototype including how we smart contracts may be leveraged to improve the agreement, tracking, and payment part of the procurement process; and, to illustrate how smart contracts might work when applied in the real world of government procurement, we will offer a notional use-case where smart contracts could be beneficial as part of a Federal Supply Schedule process.

Blockchain Technology Overview

Blockchain … Isn’t That Just Bitcoin Hype?

What is a blockchain? Believe it or not, a blockchain is pretty much exactly what it sounds like.

A blockchain is a series of blocks (or batch of transactions) cryptographically linked to one another to form a digital ledger. Each block may contain one or more transactions such as the amount of currency to exchange. A blockchain provides an immutable, transparent, irrefutable, record that is permanently stored on multiple machines or nodes. Trust between parties that may not otherwise trust one another is established through a blockchain without requiring assistance from an administrator or traditional centralized services.

To summarize, the key components of a blockchain include the following:

- P2P Protocol: the protocol that manages the peer nodes of the network that support blockchain
- Performs communication between node, flow control, node discovery, framing
- Smart Contracts (optional added feature): business rules or logic that can extend the functionality of a blockchain (Bryson et al., 2017)
- Cryptography: hash functions that link blocks together providing integrity of the chain and digital signatures providing integrity for the transactions
- Consensus Algorithm: the process by which parties to a blockchain decide on the ordering and presence of transactions on the ledger
- Distributed Ledger: a distributed, replicated, representation of all transactions

A blockchain is distributed over multiple nodes using peer-to-peer (P2P) networks. Each node within a blockchain is independent of one another and every transaction is redundantly verified and processed by every node for verification. Therefore, a single node failing on a blockchain network will not bring the whole system down as the other operating nodes can continue to run the blockchain. To compromise a blockchain, a hacker would need to have control over a large majority of the network.

A blockchain is often compared to a bank ledger containing transactions. A bank ledger records a series of transactions by collecting and reporting information. Every time a debit card is swiped at a grocery store, the bank ledger records the transaction and you'll find it next time you log into your banks app or website to review your account information. This type of ledger is traditionally done using a centralized database that is managed and stored by your bank. A database administrator oversees bank transactions which are then managed internally and reported back out for customers and other businesses to see such as the merchants bank. These transactions need to be reconciled every night.

These transactions may be changed by the bank without you having visibility into the changes themselves in real-time. For example, have you ever had a deposit hold on your debit card fall off? One day the transaction is pending, and your balance reflects this change, the next day the transaction falls off your ledger and disappears from your recent transaction list in your banks app never to be seen again. The result is that your balance is updated accordingly, but the history of the hold against the account one day and being removed the next day essentially disappears. This happens all the time with gasoline purchases, hotel stays, car rentals, and many other transactions of these types.

The blockchain solves this problem (and several others that we will discuss in more detail below) quite easily because every transaction that is written to the ledger in the blockchain is permanent so they cannot be changed or deleted. In the example of the deposit hold against the bank account, the blockchain records each transaction individually so the hold would be recorded on one day and a new block would record when the hold is removed on the next day allowing for complete transparency into the account ledger information at any point in time.

Each transaction is bundled into blocks and these blocks are linked to form the ledger, which is called a blockchain. At its core, a blockchain enables a network of peer computers (or nodes) to validate, settle, and agree on a record of transactions. It establishes a form of trust between parties that may not otherwise trust each other, and does so without relying on traditional centralized services, or trusted third parties (Bryson et al, 2017).

Centralized Databases vs. a Blockchain

Although a blockchain is a database in the form of digital ledger, a database is not a blockchain. A database is a ledger that is controlled and maintained by an administrator. The administrator can create, modify, and delete data stored in the database at any given time. The administrator can also delegate and provide rights to read or write data to other users.

A database is centralized as there is a single point of control of the data. Because of this centralized single point of control, a database is more inclined to be hacked or misused—recent revelations regarding Facebook's use of user data offers a contemporary example of what might happen when there is single point of control for your data (Lomas, 2018). According to blockchain expert Vince Tabora, "A company that has control of information can monetize it for third party use, but sometimes it is not in the best interest of users" (Tabora, 2018). Other differences (and drawbacks) of a centralized database are that since there's a single point of control of the database, a failed server will affect the entire system. Likewise, the data will not be recoverable if the information was not backed up and stored.

Traditional databases are optimized for transaction throughput. Transactions may be processed on a database in a matter of seconds while it may take several minutes for new blocks to be created on a blockchain as these new blocks work their way through each node of the blockchain.

Digital Ledger Technology (DLT) vs. Blockchain

Blockchain and DLT share common themes in that they are both decentralized and digitalized ledgers. Many people use blockchain and distributed ledger technology interchangeably, but they are vastly different.

Blockchain is a type of DLT where a series of blocks are interconnected. Each block contains data that is verified and validated before being attached to the chain of transaction records. Blockchain data is permanently stored and cannot be manipulated. There are several different types of DLT and blockchain is just one example. All blockchains are DLTs but not all DLTs are blockchains.

DLT is the "umbrella" term used to describe a database that is shared across various locations or multiple participants in a trusted environment. DLTs do not have a centralized administrator or centralized database. Like blockchain, DLT data has a timestamp that contains unalterable history of all transaction records in the network. Any of the participants on the DLT can view all the data. The data on a DLT is secure and stored using cryptography that can be retrieved with keys and cryptographic signatures (Buntinx, 2017). Comparing blockchain to DLT would be like using the analogy that a Lexus is a type of automobile (Kashyap, 2018).

Dumb Contracts vs. Smart Contracts: How the Status Quo Can Change

Dumb Contracts

Current methods for writing contracts could be described as "dumb." Often, requirements stakeholders, contracting officers, their specialists and representatives perform slow, manual, labor-intensive activities based in some form of a word document, spreadsheet, database file, or arcane contract writing system. In cases where requirements are truly unique, and customization is required, this type of approach can make some sense. However, for a vast number of the acquisitions and procurements for commercial goods and services, the process is repetitive.

Processes for contracting and acquisitions may or may not be documented within an organization leading to differences even between groups within the same office. As a result, the process may not always be 100% repeatable across an organization when buying the exact same good or service. In some cases, processes may appear to be completely digitized and have some sense of automation on the front end because of the use of a web-based interface, when in fact the backend is simply generating a slew of emails and forms that must be manually reviewed and approved to continue along in the process.

Change orders, for example, when something in the existing contract must be modified, may become tripwires that generate additional downstream churn and are often overlooked at contract initiation. These safeguards are in place to ensure taxpayer funds are spent appropriately.

Smart Contracts

Blockchain-based smart contracts enable automation of dumb contracts as noted above. Smart contracts achieve this by taking the ledger-based blockchain innovations previously discussed and overlaying some business logic on top of them enabling automatic execution when certain pre-defined terms and conditions are met. A common basic example of a smart contract is that of the vending machine whereby you insert a coin into the machine and in return the machine gives something to you. The machine is programmed to give you X when Y dollars/cents have been received. This is the business logic that has been pre-programmed into the machine. As compared with a dumb contract, in the vending machine example, the transaction occurs without the presence of a middleman. By comparison, when you go into a gas station convenience store and must walk up to the counter and hand the clerk the soda and your money in order to check out, the clerk is the middleman who must be present for you to complete the transaction. Moreover, if you happen to use a debit/credit card to purchase the soda in the store, the merchant’s credit card processing company and your bank or credit card issuer act as additional middlemen who must all be present for the transaction to be processed. By comparison to the “smart contract” vending machine example, if paying in cash, the transaction is solely between you and the machine itself because the machine has been preprogramed to dispense a soda once the correct amount of money has been deposited—no middleman required.

Smart contracts may be useful for purchasing basic goods and services and may also be beneficial for things like insurance policies, breach contracts, property and real estate transactions, issuing and managing credit, financial services, legal processes and crowdfunding agreements among others where typically the services of a middleman have been previously required (Blockgeeks, n.d.).

Benefits of Smart Contracts

Smart contracts offer numerous benefits that can be realized across the government acquisition and procurement process which are discussed in more detail below:

- **Autonomy—**Smart contracts allow the creation of a direct agreement between two parties without use of an intermediary. Moreover, because there isn’t an intermediary the transaction may not be manipulated by a third-party.
- **Trust**—Smart contracts permit trust to be built into the process because all information and associated documents/data are encrypted on a shared ledger, so they cannot be lost.

- **Backup**—Because the blockchain stores information related to an agreement on the shared ledger across a distributed network, there will be multiple copies of stored information.
- **Safety**—The blockchain is secured through cryptography; blockchain relies on two cryptographic primitives to help secure the chain—digital signatures and cryptographic hash functions. Both are used to verify and ensure the integrity of data.
- **Speed**—Smart contracts can automate tasks if business logic is pre-defined and built into the blockchain, as a result, previous tasks related to contracting that were done manually (such as quality reviews or multiple approvals) could be executed automatically.
- **Savings**—Smart contracts have the potential to save considerable amounts of money as intermediaries are no longer necessary. Moreover, business process improvement may be possible after the introduction of smart contracts in parts of the process where redundancy to include multiple human approvals was built in to explicitly improve trust, safety, and accuracy.
- **Accuracy**—Automated contracts avoid the errors that come from manually filling out endless amounts of paperwork like spreadsheets and word documents. If the appropriate business logic is built into the smart contract, only those spreadsheets or documents that meet the pre-defined accuracy criteria would be accepted (Blockgeeks, n.d.).

Drawbacks of Smart Contracts

The term *smart contract* is a bit misleading, as they are not inherently “smart” nor a “contract” in the legal sense. Smart contracts are essentially the business logic of the blockchain that run during blockchain transactions and are only as good as the logic programmed in to them. Smart contract functionality varies by platform as each may offer differ capabilities. However, in all cases the blockchain cannot prevent programmer error. So due diligence is needed to prevent introducing security problems via a smart contract. Additionally, it’s very important that smart contract logic executes in a deterministic fashion, whereby outcomes are precisely determined through known relationships among states and events as this plays a key role in the network reaching consensus on a given set of transactions.

Blockchain Smart Contracts Prototype: Agreement, Tracking and Payment in Action

MITRE’s research in applying Blockchain technology is focusing on three high-level areas that apply to acquisition and procurements: Agreement, Tracking, and Payment. We’re exploring how blockchain technology coupled with smart contracts may help to improve the efficiency and integrity of the process across these areas. Nearly all business processes rely on these areas to conduct day to day activities. We are building small prototypes in an incremental fashion. Our goal is *not* to build a production level system., but rather to demonstrate and evaluate the potential capabilities of blockchain and smart contracts as applied to the areas of agreement, tracking, and payment within acquisition as defined below.

- **Agreement:** Can we automate the process of establishing an agreement among parties without relying on centralized control or services? Why is this important? Agreements are used to establish trust among parties as well to enforce policy and procedures. In our use-case, this involves several documents related to approvals, terms and conditions when the government is procuring a good or service. Integrity and efficiency can be improved by eliminating the need for centralized control to enforce and process these agreements, along with automating the rules and verification via cryptography.

- **Tracking:** Every organization involved maintains their own system of record, yet parties to the contracting process, often need to have a shared view into the overall state of a given agreement or transaction. Sharing this information across organization boundaries via traditional technology has been a pain point for decades. Blockchain technology is very good at providing a tamper-resistant, audit logic that can be safely shared among all parties internal and external to the government.
- **Payment:** Moving money around and across governmental organizations and outside of government to pay vendors requires many checks and balances. If we could employ digital currency in the Enterprise, it may be able to streamline processes by eliminating spreadsheets and reconciliation services.

Current Blockchain Smart Contracts Prototype Achievements

Since the beginning of FY19 through date of this research, the prototype has demonstrated the following:

a. An agreement is created and processed. We use a blockchain and smart contracts to capture, track, and enforce the rules of an agreement. We use decentralized file storage to store the traditional documents associated with an agreement. The decentralized file storage also maintains a unique fingerprint of each document to ensure parties are collaborating on the correct version of an agreement—no more emailing documents around while trying to track the right version via the filename.

b. A cryptographic "wallet" was created for every user who intends to interact with the system. Any transaction sent to the system to digitally sign an agreement, assign a funding authority, etc., requires a cryptographically signed transaction from that user. The signature is checked several times by every permissioned validator node to verify the user before the transaction is accepted. This increases the integrity of the transaction and the transaction is permanently stored in the blockchain for auditability.

c. A decentralized notary service was established to verify, and process digital signatures required by the documents associated with the process. The notary service is implemented as a smart contract ensuring the integrity and authenticity of signatures simplifying the document approval process.

d. A rules-based flow was established to enforce the agreement through the process:

    i. User creates a request for purchase along with required signers.

    ii. When all signers have signed a funding authority is assigned by their cryptographic wallet address. Once the associated funding doc(s) are signed, the funding transfers the funding amount (in digital currency) to the selected contracting office.

    iii. The contracting office develops an RFQ and opens the process for bidding. Once the bidding process ends. The "best" bid is selected, and the winning bidder is recorded in the smart contract agreement.

iv. The contracting office then “pays” the winner bidder for the service via digital currency over the blockchain

v. When the purchase is received, creator of the agreement “closes” the agreement.

Using the approach, the entire process agreement generation, document signatures, money transfers, and so forth, are recorded on the blockchain in an immutable, auditable ledger and available for all parties to the process to examine.

Applied Use Case: How Smart Contracts Prototype Could be Implemented in the Government

The intent of this use is to examine how our prototype could be applied to a simple acquisition of standard Commercial Off-the-Shelf (COTS) software licenses using a Federal Supply Schedule.

This use case is organized in the following manner: a general introduction to the Federal procurement process, an example requirements generation process that describes the status quo, how smart contracts could be used, and potential benefits; an example contracting process that describes the status quo, how smart contracts could be used, and potential benefits; applicability of this use case; barriers to a smart contracts prototype implementation; keys to success for a smart contracts prototype implementation; and, a short conclusion.

Understanding the Federal Procurement Process

When an individual or an organization has an immediate need to procure a COTS item, such as geographic information system (GIS) mapping software, the process is simple enough. The individual consumer or corporate purchasing agent simply logs into the software sales point of entry, clicks on the subscription or product that best meets their needs, inputs their registration and payment information, and downloads the software. The process generally takes less than an hour. Conversely, when a government information technology (IT) specialist needs a similar piece of software, the process to fulfill that need could not be more different. Instead of going through an automated online purchase transaction, the IT specialist is directed to a much more subjective acquisition process, which could take up to 90 days to complete. This leads us to the following question: How might we introduce blockchain-based smart contracts to improve the procurement of COTS software?[1]

While the detailed nuances for procuring COTS software differs from agency to agency, the overall federal procurement process is relatively fixed. Below is a representative example of the wickets that an agency would have to navigate in order to acquire software licenses. For clarity’s sake, this process is broken down into two major groups: Actions of the Requiring Activity/Customer and Actions of the Contracting Team (see Table 1).

[1] While this process could be customized for federal COTS procurements at any dollar level, this particular case study process is focused on those software purchases between the ranges of the FAR Micropurchase Threshold and the Simplified Acquisition Threshold.

Table 1. Actions of the Requiring Activity/Customer and Actions of the Contracting Team

Actions of the Requiring Activity/Customer
Step 1. Determination of Requirements
Step 2. Seek Requirements Validation
Step 3. Secure, Commit, and Transmit Funds
Step 4. Transmit Requirement Package to Contracting Officer (CO)

Actions of the Contracting Team
Step 1. Review Package for Sufficiency
Step 2. Prepare the Request for Quotation (RFQ)
Step 3. CO Seeks RFQ Approvals (Legal, Policy, Manager, Peer Review) Step 4a. Post RFQ on eBuy Step 4b. Transmit RFQ to Specific Vendors Step 5. Receive Quotes
Step 6. Evaluation of Quotes
Step 7. Award Decision
Step 8. Award Notification
Step 9. Tracking Contract Performance
Step 10. Contract Payment
Step 11. Contract Closeout

This standard process for procuring simple commercial items or services follows many of the same steps as the procurement of more complex solutions or services. While this process may be scaled down somewhat for more “simplified acquisitions,” this approach is far from efficient. Upon quick review, the process is inefficient; requires unnecessary reviews and/or approval from members with little or no equity in the acquisition; and adds unnecessary schedule delays.

By automating those functions that can be processed using machine logic, the government should be able to realize the following second and third order effects:

- Reduction in the number of “touch points” needed to process a simple COTS acquisition,
- Greater standardization and simplification of requirements inputs to include requirements definition, cost estimating, market research, and evaluation of quotes,
- Reduced number of resources (i.e., employee hours) needed to execute the transaction through the reduction of said “touch points” listed above,
- Improved procurement acquisition lead-times,
- Faster delivery of software products and support services,
- Quicker processing of payment, and
- Automated enforcement of the process flow including redundant verifications.

So, how could we apply a blockchain-based smart contracts approach to this use case? The critical piece of this analysis starts with a detailed examination of the current procurement steps and analyzing each to see which, if any, steps can be automated—comfortably replacing human decisions with machine logic.

Requiring Activity Steps

Let’s start by examining the first four steps executed by the Requiring Activity or Customer.

Step 1. Determination of a Requirement

One of the most difficult challenges in the area of procurement is the task of defining contract requirements. Traditional processes require the requiring activity to draft a Statement of Work (SOW) document identifying required salient characteristics that allow for multiple vendors to respond with formal quotes. Requirements definition is one of the primary points of contention between a contracting office and its customers, often resulting in numerous significant back-and-forth iterations of work statement reviews.

We recommend establishing an agency pre-approved menu of software license solutions available for the IT professional to select. The process of developing a work statement would essentially be replaced by completing an eForm requisition, which would include: a description and quantities of the license(s) requested; overall estimated cost; a list of sources and other simple market research data points; a short narrative or justification explaining why the software license is required; and a narrative/list of the equipment on which it would be installed.

By consolidating all these data points onto one eForm, we essentially eliminate the requirement to draft a Statement of Work (SOW), Independent Government Cost Estimate (IGCE), Market Research Report, and an agency needs justification document. This eForm would be certified by the preparer and would initiate the procurement process in the blockchain.

Step 2. Seek Requirements Validation/Approval from Agency (Processes Vary by Agency)

Once a purchase request is initiated, there is often an internal agency review process. This requirements validation process is established with the intent of ensuring that the need is valid, the requirement is an appropriate use of agency funds, and that the request agrees with the policies of that agency. It is not uncommon for this requirements validation process to be top-heavy and lengthy. In many cases, the process involves multiple layers of unnecessary approvals with final approval levels being established at the highest executive levels (who often have very limited schedule availability). The higher the approval authority that is established, the greater the number of people that review the requirement prior to final approval. Further, some organizations only perform this requirements validation process on a semi-annual or quarterly basis, adding even more time to the process. While this level of scrutiny may be appropriate for multi-million-dollar requirements, it would not be appropriate for simple low-dollar COTS software purchases.

To address this, we recommend establishing a blockchain-based smart contract with pre-defined business logic that automates the approval process for all requisitions to a Chief Information Officer (CIO) representative within the organization for approval if the requisition is (1) for a COTS software solution; and (2) under a pre-determined price threshold that the organization can accept as low-risk. Replacing a multi-layered requirements validation process with an automated step that is executed by the pre-programed smart contract, could reduce the procurement lead time by weeks and even months by eliminating the number of non-value-added reviews as often the degree of human checking is not proportionate with the dollar amount or complexity of the transaction.

Step 3. Secure, Commit, and Transfer Funding to Contracting Office and Step 4. Transmit Approved Requirements Package to the Contracting Officer

After a requirement is validated and approved, the next step is normally to secure, certify and transmit funding to the contracting office. In the traditional procurement process, this requires the customer to prepare a “purchase request” for funds, which would then circulate through a series of reviewing/approving steps before a representative with “commitment” authority certifies that funds are “available” for this procurement and provides a unique accounting code for the purchase. Once the funds are “certified,” the procurement package is routed to the contracting office manually or electronically through email or another pre-approved agency system.

Again, this is a task that can be automated into a smart contract process. In this case, once the requirement is validated, the task would move to the next step, which would require the system ensure the correct funding account was being selected and would perform a comparison of the anticipated requirement cost vs the available budget and/or some other pre-determined approval dollar threshold. If the cost is less than both and the correct account was selected, the process could move forward to funds certification. In other words, the agency could set pre-established conditions (built in to the blockchain-based smart contract as business logic) under which the process could proceed without human interaction, until it reaches the final stage of “funds certification.”

Because of the low-dollar amount of the requirement, the number of reviews could be reduced by introducing machine review gates into the smart contract business logic, which would validate funds being applied were of the appropriate time, purpose and amount required. The funds would then be forwarded to the funds certifying official in the blockchain for review/approval. Approval of these funds would then trigger the next automated step—Transmittal to the Contracting Office.[2]

Contracting Team Steps

Step 1. Review Requirement Package for Sufficiency

Once the customer submits the requirements package, the contacting office becomes the lead for further processing and facilitates the steps provided below.

Acceptance of a requirements package is often a hot spot in the procurement process. A primary reason for this friction is that the “clock” for Procurement Acquisition Lead Time (PALT) officially starts once the requirements package is accepted by the contracting office. This creates an environment where there is a reluctance to accept weak or incomplete requirements packages. Contracting offices will often reject the package and require the customer resubmit with corrections or improvements.

This need not be the case in a procurement as simple as the purchase of a COTS license. Assuming the IT specialist complied with the initial guidance, completed the

[2] Note: Federal agencies utilize numerous different processes and/or systems to track and certify funding. In order to integrate blockchain and smart contracts into this process, they would have to interface with those systems. Alternatively, the funds certification process could be performed outside of blockchain, and then integrated back into the process once funds are approve.

eForms/requisitions correctly, received adequate requirements validation, and secured enough certified funding, the acceptance of a procurement package should be easy to validate through pre-defined smart contract business logic that captures the specific requirements necessary for a complete requirements package to be permitted to move forward.

By standardizing and automating the required inputs of the requirements package, the acceptance process is made significantly easier. The contracting officer task of performing a complete procurement requirements package review (which includes the SOW, purchase request (PR), IGCE, Market Research Report, requirements validation, and funds certification) is instead reduced to a more simplified review of the completed requisition eForm, the simplified requirements validation, and the certification of funds.

Step 2. Prepare the RFQ

By standardizing and automating the required inputs of the requirements package, the acceptance process is made significantly easier. The contracting officer task of performing a complete procurement requirements package review (which includes the SOW, PR, IGCE, Market Research Report, requirements validation, and funds certification) is instead reduced to a more simplified review of the completed requisition eForm, the simplified requirements validation, and the certification of funds.

Once the contracting officer has accepted the requirements package, the contracting team prepares a Request for Quotation (RFQ) for distribution to the potential offerors. Depending on the details of the requirement, this RFQ can be prepared using a government form (i.e., SF 1449 or DD 1155), a formal letter, an email, or even an oral request over the phone.

As mentioned previously, this use case capitalizes on the use of Federal Supply Schedules to procure the said software licenses. One of the greatest benefits of utilizing Federal Supply Schedules is that all the terms and conditions are pre-negotiated and automatically wrapped into the price of the software. This allows the government to focus almost exclusively on price for the individual order. Because we are using these schedules, the RFQ can be dramatically simplified using a standard fillable letter or email. This process could be easily automated by the smart contract pre-populating a standard RFQ form letter with the information provided in the original requisition eForm and a few additional inputs. Unlike other more complex solicitations, all the clauses, provisions and other terms for the RFQ are already pre-defined under the governing schedule.[3] Using this approach, the system could easily generate an RFQ by populating a form simple letter utilizing standardized automated inputs.

Step 3. Seek RFQ Approval From Contracts Chain (Legal, Policy, Manager, Peer Review)

Many contracting offices require multiple layers of review before a solicitation is released to potential bidders. Normally, the RFQ is prepared by a contract specialist and reviewed by the contracting officer. However, some organizations require additional

[3] Note, some organizations such as the DoD have mandatory specialized clauses in addition to the pre-negotiated GSA terms and conditions. In such cases, these additional terms can be added to the RFQ eForm.

solicitation reviews from independent peers, branch supervisors, policy teams, and legal counsel. These reviews could add weeks to the procurement process.

We recommend that the review requirements be minimized as much as possible, especially in cases such as this where the acquisition is simple, low-dollar, and utilizes pre-established Government-Wide Acquisition Contracts (GWACs). However, if additional RFQ reviews are required, this process could be greatly simplified and expedited by establishing a "Smart Contracts Analyst" who would be specially trained to perform compliance reviews with a focus on issues related to COTS acquisitions using a blockchain-based smart contract with pre-defined business logic. These reviews, adjudications, and approvals would be recorded transactions on the blockchain with the supporting data being stored in decentralized file storage. Once all compliance approval is received and all concerns are adjudicated, the contracting officer/contract specialist can proceed to the next step—transmitting the RFQ to vendors.

Step 4a. Post RFQ on eBuy IAW FAR 8.405-1(d)(3)

Step 4b. (Alternate to 4a above) Transmit RFQ to Specific Vendors

Step 5. Receive Quotes

The rules for procuring solutions under the Federal Supply Schedules is uncharacteristically explicit. The Federal Acquisition Regulation specifically outlines the contracting officer's processes and requirements under subpart 8.405-1, Ordering Procedures for Supplies and Services Not Requiring a Statement of Work, and further explains the required procedures under subparagraph (c), Orders exceeding the micro-purchase threshold but not exceeding the simplified acquisition threshold. Under this section, the FAR states that the agency shall survey at least three schedule contractors through the GSA Advantage! online shopping service by:

- Reviewing the catalogs or pricelists of at least three schedule contractors. An automated process can be established to collect pricelists from GSA Advantage to assist determining which vendors offer the most competitive pricing. Machine logic can then be applied to compare prices to each other.
- Requesting quotations from at least three schedule contractors. If the contracting officer elects to solicit multiple quotes, the transmittal of an RFQ to one or multiple GSA vendors can be achieved through automated systems using blockchain to record the transmittal. Not only would blockchain record the transmittal of the RFQ, but it would also provide a tamper-proof method to certify (i.e., date stamp) when that transmittal occurred by building such business logic into the smart contract.
- Posting the RFQ on GSA's competition web platform and seek responsive quotes through that eBuy portal (FAR 8.405-1(d)(3)(i)). If the contracting officer elects to solicit quotes from all GSA schedule holders through the use of the GSA eBuy system, the RFQ that is transmitted could include explicit instructions for offerors to submit their quotes to the government through a method or system that is also recorded on the blockchain.

Once vendors have the opportunity to review the RFQ and prepare their quotes, those vendors would then transmit their offers to the contracting office utilizing the prescribed blockchain-based system, which would leverage the pre-defined smart contract business logic to record the transaction and assign a date/time stamp as proof of submission.[4] For ease of processing and evaluation, the government could require that the quote be provided through automatically populating a pre-established eForm again based on pre-determined smart contract business logic.

Step 6. Evaluation of Quotes

Step 7. Award Decision

A traditional federal procurement process normally goes through a manual evaluation and decision-making process. This process involves multiple components:

- A review to determine if the offer is "responsive" (i.e., meets requirements of the RFQ);
- A technical review of the offer to ensure proposed solution meets the technical requirements of the RFQ; and
- A review of price.

If the quotes are prepared in accordance with the standards set forth in the RFQ and the required eForms, Step 6, Evaluation of Quotes, and Step 7, Award Decision, should be relatively straight forward and easy to complete. The quotes would be provided in a manner that allows the smart contract business logic to compile the information, to filter out non-compliant quotes, and to compare "apples to apples." Lastly, evaluations and awards could be further simplified by building in the template the smart contract business logic that can provide the contracting officer with quotes that are pre-organized for ease of analysis and automatic export into an award decision document that has also been built into the pre-determined smart contract business logic.

By automating the requirements package inputs, the RFQ, and the mandatory structure of the quotes, the information can be screened, consolidated, and organized in a manner that allows the contracting officer to simply validate the information and certify the award decision result.[5] This result would also be recorded on the blockchain and the associated files would be archived in distributed storage. This step would also include the contracting officer's task of preparing the award document. Normally the award document would be prepared using government forms SF 1449 or DD 1155, which are generated utilizing federal contracting systems, outside of the smart contract construct. Once the award is executed in the government contracting system, the award document could be extracted and fed back into the blockchain. It may also be possible to integrate directly into the government contracting system depending on the nature of the interfaces and technical architecture.

Step 8. Award Notification

Once the contracting officer receives internal approval and signs the contract, he/she would traditionally transmit that contract to the awardee via email. Similarly, all unsuccessful offerors would receive a letter via email notifying informing them that they were not selected

[4] Note: this is a particularly useful feature when there are questions regarding the timeliness and acceptability of the offeror's quote.

[5] This assumes the contracting officer adopts a "lowest-price technically acceptable" selection approach, which is highly compatible with the procurement of COTS.

for award and providing them with pertinent information (i.e., name of awardee, amount of award, etc.).

The process of Award Notification involves nothing more than the transmittal of information—a process that a blockchain-based smart contract can be easily designed to support with the corresponding business logic built-in. Once an award decision is made by the contracting officer, that information could be quickly processed using smart contract business logic in the form of a template/letter notifying all interested parties of the selected awardee and relevant award information. The information would be transmitted, and delivery would be recorded on the blockchain providing the government an error free proof of receipt. This approach saves the government time in preparing award notification, and instead allows the contracting officer to focus on his or her review responsibilities, rather than getting bogged down in administrative tasks that can be executed as part of the smart contract's automated business logic.

Step 9. Tracking Contract Performance

Step 10. Contract Payment

Since this use case involves the procurement of a software solution, the government function of tracking performance is greatly simplified. The actual software license generally is treated as a supply purchase, and performance is met when the software is delivered. The ongoing software support services (i.e., patches, help desk, troubleshooting support) is normally treated as a subscription. As with delivery of software, the support subscription is typically considered complete and payment is made when the subscription services are initiated. No long-term contractor performance surveillance is required for the follow-on upgrades, patches, and help desk support. Agencies utilize multiple methods for certifying delivery. Most agencies use electronic systems such as the DoD's Wide Area Workflow (WAWF) System to certify when delivery occurs, which triggers an authorization to make payment.

As stated above, the oversight and payment processes are already highly automated. As such, a blockchain-based smart contracts approach would have to be fully integrated into these existing systems in order to record those activities. Alternatively, a new system could be implemented which could automatically track delivery of software and support services with the vendor notifying the government when both were provided (like the smartphone app used by Amazon). The government could utilize this same system to confirm receipt and authorize payment utilizing a Government Purchase Card rather than electronic funds transfer. All transactions would be recorded on the blockchain and executed based upon the pre-defined business logic built into the smart contract for the software. This approach would require special authorizations and would likely have to meet or exceed the requirements of the Prompt Payment Act of 1982 (FAR 12.301(b)(3) and FAR 52.212-4).

By utilizing a smart contracts approach and the use of the Government Purchase Card, payment could be made automatically within hours of receipt of the software and subscription services, rather than some 30 days later. This would be much more in-line with commercial best practices and would encourage the vendor to offer more competitive pricing to the government as well as reduce risk of incurring interest penalties. Moreover, this would reduce the burden to smaller or other non-traditional government vendors who simply can't wait a month to get paid for a good or service that has been delivered and accepted by a customer.

Step 11. Contract Closeout

Finally, after the transaction is fully completed, all goods are provided and services are received, the contracting office is normally required to “closeout” the contract for archiving and eventual destruction. In many offices, this is performed utilizing a manual process. Specifically, a government employee or contractor will review the contract and determine if there are any outstanding disbursement balances. If all payments have been made, the employee will prepare a close-out document for contracting officer approval and add it to the contract file. If outstanding unpaid balances exist, the file is set aside for further resolution.

Many organizations already have an automated closeout process for simple, low-dollar acquisitions. This type of transaction could easily be applied by building the closeout process into the smart contract business logic. The simple smart contract agreement could consider easily programable syntax questions whereby the answers have already been recorded as previous transactions on the blockchain such as the following:

- Final payment made (Y/N)?
- Outstanding/undispersed funds(Y/N)?
- Any outstanding performance issues(Y/N)?
- Is it now 30 days or greater beyond performance end-date (Y/N)?

By applying this process, the government would no longer have to manually review each file. Instead, they could focus on only those files that need special adjudication, saving both considerable time and resources.

Applicability of This Use Case

As shown above, the employment of blockchain-based smart contracts could greatly improve the trust, autonomy, and security within a simple procurement of software licenses under Federal Supply Schedules. Once greater trust, autonomy, and security are introduced into the procurement system, it permits business processes to be re-engineered purposefully to reduce the redundancy and inefficiency. As described, such inefficiency is often built-in as a result of the numerous errors that occur in a manually driven, centrally managed environment. Speed, accuracy, and efficiency all become second order benefits realized upon the blockchain paradigm shift once embraced by the organization.

Can this approach be used to procure software outside of Federal Supply Schedules? The simple answer is yes. Use of the above discussed blockchain-based smart contracts process can be leveraged in procuring COTS when utilizing other software GWAC vehicles.

One of the first examples for additional consideration to implement blockchain-based smart contracts is the DoD’s family of Enterprise Software Agreements (ESAs) which provide a full complement of pre-negotiated COTS blanket purchase agreements (BPAs) to provide Remedy, Adobe, Redhat, SAP, and numerous other software and support solutions.

Another primary source of COTS for civilian federal agencies is NASA’s Solutions for Enterprise-Wide Procurement (SEWP) V GWAC, providing a full complement of IT commercial software products through multiple-award Indefinite Delivery/Indefinite Quantity (IDIQ) contracts. In both cases, a similar approach can be used to build, validate and fund the requirements package, as well as execute many of the same contracting process steps outlined in this case using machine-logic.

Barriers to Implementation of the Smart Contracts Prototype

As with any proposed innovative solution, there are often obstacles that need to be overcome for successful implementation. The following is a discussion of three potential barriers to employing this technology in a federal acquisition environment.

- **Contracting Officer Discretion.** It must be acknowledged that by its very nature contracting absolutely must involve the business judgement of a warranted contracting officer. If the government were to develop a blockchain-based smart contract system to procure simple goods and services, it cannot (at least in the short term) replace automated business logic built into smart contracts with individual contracting officer judgement in a few key areas: Determination of Acquisition Strategy; Determination of the Best Value of the Government; and Final Selection of the contract awardee. All these determinations are inherently governmental, reside exclusively with the contracting officer, and must be completed before he/she will make a contract award obligation on behalf of the government. Accordingly, any established blockchain-based smart contracts process must make room for contracting officer discretion in the award process for procurement of software.

- **Brand Name and Related Competition Concerns.** The FAR spends considerable time laying out special rules and processes for acquiring "brand name" solutions (See FAR 6.302-1(c), 8.405-1(e), and 8.405-6(b)), which requires requiring activities to explicitly identify and justify those "salient characteristics" associated with the "brand name" product in order to foster a more fair and just competitive environment. This issue is especially pronounced when multiple firms produce a COTS product that is of a similar type. For instance, there are multiple COTS solutions that provide security protections for laptops (i.e., Symantec, McAfee, Kaspersky, Bitdefender). The FAR normally prohibits the customer from arbitrarily selecting their preferred product. Instead, the FAR requires the government to define the salient characteristics needed for that software (in this case security software) and allows the entire segment of industry to compete in the RFQ. Unless Congress is willing to relax the requirements of the brand name restriction, this will remain an impediment to simplifying Step 1, Determination of a Requirement. The smart contract business logic could be programmed to leverage previous software contract performance characteristics as part of the process to generate a new agreement.

- **Scale.** The point of employing blockchain-based smart contracts into acquisition of software process is to realize organizational efficiencies and savings that come with improving trust, autonomy, and security in the process. It must also be recognized that building a blockchain-based smart contract solution also requires government resources. The agency exploring the use of this solution should perform a cost/benefit analysis to determine if the return (benefits achieved in software acquisition) are worth the investment (resources needed to build the system). While the return on investment (ROI) results will vary for each agency, one common premise exists—the scale of the software requirement(s) is determinative. In other words, the greater the scale for COTS software need across a department, agency or government-wide, the more benefit that a blockchain-based smart contracts solution provides.

- **Legal Concept of Remedy.** If something goes wrong in paper based legal system, the "remedy" is very malleable. In a blockchain-enabled world, the "remedy" is a set of additional blockchain transactions. This requires an updated mindset, and a blockchain-enabled capability that can distinguish between the original transactions, recognition of an issue, and the remedy transactions.

Conclusions and Recommendations for Successful Implementation of the Smart Contracts

It is unlikely that the government will ever be able to make the software acquisition process completely mirror industry best practices. However, tremendous progress can be made in working towards achievement of that goal by improving trust, autonomy, and security in the process that can ultimately result in improved efficiency and cost savings for the government.

In order to make the successful implementation of blockchain-based smart contracts, there are several special considerations related to software acquisition that need to be in place. First, the agency needs to have access and authority to utilize enterprise-sized software acquisition vehicles to achieve savings through economies of scale such as the GSA's IT 70 or the DoD's ESAs. It's not enough to make the existing in-house process simpler as a result of the introduction of blockchain technology that adds trust, autonomy and accuracy to business operations which will ultimately yield greater efficiencies and cost savings.

Second, the efficacy of using a blockchain-based smart contract solution would be increased significantly if, in the requirements development step, the customers are able to select COTS solutions that are pre-approved by the agency for use and are not be required to develop a list of "salient characteristics" needed for software procurement. In other words, the agency needs to establish pre-competed COTS solutions for agency use within software segments of competing vendors (i.e., Symantec vs. McAffe, ArcGIS vs. Geosoft, Tableau vs. Lumira). By establishing agency-wide pre-selected/pre-competed solutions, the government enables more standardized contracting requirements, as well as terms and conditions that can be built into the smart contract business logic.

Third, establish pre-set requirements needed to receive software validation approval which can be built into the smart contract business logic. Organizations may be compelled to procure software for an entire group of people, even though only a small subset of users require it. Normally, this rationing or scrutiny is applied during the validation step. In order to make this step go much smoother, it would help if the agency CIO publish pre-established screening criteria or other thresholds that must be met in order to receive requirement validation approval. Without clear, definitive guidance on what "will or won't fly" with the CIO, customers may unwittingly be wasting their time seeking validation of their software request. With clear guidance from the CIO representative, this ambiguity is reduced or eliminated.

References

Arrietta, J., & Hager, T. (n.d.). HHS emerging technology. Retrieved from https://www.actiac.org/system/files/ACT-IAC HHS Emerging Technology Day.pdf

Bahuguna, A. (2018, July 24). Blockchain smart contract security—Blog by Saama. Retrieved from https://www.saama.com/blog/blockchain-smart-contract-security/

BBVA. (2018, April 26). What is the difference between DLT and blockchain. Retrieved from https://www.bbva.com/en/difference-dlt-blockchain/

Belin, O. (n.d.). The difference between blockchain & distributed ledger technology. Retrieved from https://tradeix.com/distributed-ledger-technology/

Blockgeeks. (n.d.). Smart contracts: The blockchain technology that will replace lawyers. Retrieved from https://blockgeeks.com/guides/smart-contracts/

Bryson, D., Goldenberg, D. C., Penny, D., & Serrao, G. (2017). Blockchain technology for government. Montgomery, AL: The MITRE Corporation.

Buntinx, J. (2017, March 25). Distributed ledger technology vs blockchain technology. Retrieved from https://themerkle.com/distributed-ledger-technology-vs-blockchain-technology/

Centralization vs. decentralization. (n.d.). Retrieved from https://blockchain.wtf/what-the-faq/centralization-vs-decentralization/

Chesebro, R. (2015, February). A contract that manages itself. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a620401.pdf

Choudhury, O., Sarker, H., Rudolph, N., Foreman, M., Fay, N., Dhuliawala, M., … & Das, A. (n.d.). Human subject regulations using blockchain and smart contracts. Blockchain in Healthcare Today. Retrieved from https://doi.org/10.30953/bhty.v1.10

De, N. (2017, October 24). HHS architect talks blockchain's potential role in healthcare administration. Retrieved from https://www.coindesk.com/hhs-it-architect-talks-blockchain-white-paper-results?amp

DeBreuck, F. (2018, July 5). The core principles of smart contracts. Retrieved from https://www.openaccessgovernment.org/the-core-principles-of-smart-contracts/47369/

Dikusar, A. (2017, October 17). Smart contracts: Industry examples and use cases for business. Retrieved from https://xbsoftware.com/blog/smart-contracts-use-cases/

Dimov, D., & Juzenaite, R. (2016, August 17). Security of smart contracts. Retrieved from https://resources.infosecinstitute.com/security-smart-contracts/#gref

Dobesh, S. (2017, November 14). Blockchain for additive manufacturing to optimize DoD supply chains. Retrieved from https://www.gbaglobal.org/blockchain-additive-manufacturing-optimize-dod-supply-chains/

Federal Acquisition Regulation (FAR), 48 C.F.R. 12.301 (2019).

Federal Acquisition Regulation (FAR), 48 C.F.R. 52.212-4 (2019).

Federal Acquisition Regulation (FAR), 48 C.F.R. 6.302-1 (2019).

Federal Acquisition Regulation (FAR), 48 C.F.R. 8.405-1 (2019).

Federal Acquisition Regulation (FAR), 48 C.F.R. 8.405-6 (2019).

Frank, J., Newhard, A., & Silverstein, S. (2018, October 3). How smart contracts will work. Retrieved from https://www.businessinsider.com/how-smart-contracts-can-work-2018-10

Friedman, S. (2017, September 21). GSA looks to blockchain for speeding procurement processes. Retrieved from https://gcn.com/Articles/2017/09/21/GSA-looks-to-blockchain-for-procurement.aspx?m=1

GitHub. (n.d.). Awesome smart contracts. Retrieved from https://github.com/Overtorment/awesome-smart-contracts

Greenspan, G. (2016, March 17). Blockchains vs. centralized databases. Retrieved from https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/

GSA. (2019, February 26). Blockchain. Retrieved from https://www.gsa.gov/technology/government-it-initiatives/emerging-citizen-technology/blockchain

Hayzlett, J. (2018, February 15). 3 major industries in which blockchain technology is changing life as we know it. Retrieved from https://www.entrepreneur.com/article/308987

Hertig, A. (n.d.). How do ethereum smart contracts work? Retrieved from https://www.coindesk.com/information/ethereum-smart-contracts-work

Department of Health and Human Services (HHS). (2018, March 13). HHS announces health data provenance challenge winners. Retrieved from https://www.hhs.gov/about/news/2018/03/13/hhs-announces-health-data-provenance-challenge-winners.html

Jeremy, Y. (2017, August 24). DoD eyes blockchain technology to improve cybersecurity. Retrieved from https://www.dlt.com/blog/2017/08/24/dod-eyes-blockchain-technology-improve-cybersecurity/

Johnson, D. B. (2018, January 3). Will 2018 be the year for blockchain for government? Retrieved from https://fcw.com/articles/2018/01/03/blockchain-goverment-hype-reality.aspx?m=1

Kariuki, D. (2018, April 13). Blockchain use-cases in enhancing government services. Retrieved from https://www.cryptomorrow.com/2018/04/13/blockchain-use-cases-in-enhancing-government-services/

Kashyap, R. (2018, July 31). DLT vs. blockchain. Retrieved from https://cryptodigestnews.com/dlt-vs-blockchain-a4f7b97f8b2c

Kendall, F. (2014, September 19). Better buying power 3.0 [White paper]. Retrieved from http://www.acqnotes.com/Attachments/Better-Buying-Power-3.0-White-Power.pdf

Kirkman, S. S., & Newman, R. (2017). Using smart contracts and blockchains to support consumer. Retrieved from https://csce.ucmss.com/books/LFS/CSREA2017/GCC3688.pdf

Lomas, N. (2018, March 27). Zuckerberg refuses UK Parliament summons over Fb data misuse. Retrieved from https://techcrunch.com/story/facebook-responds-to-data-misuse/

Martin, Z. (2016, February 11). Blockchain partnership, GSA deploys identity-monitoring tool. Retrieved from https://www.secureidnews.com/news-item/blockchain-partnership-gsa-deploys-identity-monitoring-tool/

McConaghy, T. (2017, July 15). Blockchain infrastructure landscape: A first principles framing. Retrieved from https://medium.com/@trentmc0/blockchain-infrastructure-landscape-a-first-principles-framing-92cc5549bafe

Mearian, L. (2018, February 14). IBM sees blockchain as ready for government use. Retrieved from https://www.computerworld.com/article/3254202/ibm-sees-blockchain-as-ready-for-gover

Moehrke, J. (2016, August 29). Blockchain and smart-contracts applied to evidence notebook. Retrieved from https://healthcaresecprivacy.blogspot.com/2016/08/blockchain-and-smart-contracts-applied.html?m=1

Nayak, N., & Nguyen, D. T. (2018, March 27). Blockchain, AI and robotics: How future tech will simplify federal procurement. Retrieved from https://www.federaltimes.com/acquisition/2018/03/23/blockchain-ai-and-robotics-how-future-tech-will-simplify-federal-procurement/

Nene, V. (2018, October 19). Smart contracts for drones using blockchain. Retrieved from https://dronebelow.com/2018/10/19/smart-contract-for-drones-using-blockchain/

Novak, M. (2017, September 22). Blockchain & smart contracts for government entitlements & payments. Retrieved from https://www.slideshare.net/MichaelNovak9/blockchain-smart-contracts-for-government-entitlements-payments

Ozelli, S. (2018, January 23). US government implements blockchain programs to improve transparency and efficiency: Expert blog. Retrieved from https://cointelegraph.com/news/us-government-implements-blockchain-programs-to-improve-transparency-and-efficiency-expert-blog

P., H. (2018, July 12). Smart contracts use cases and examples in blockchain (Simple guide). Retrieved from https://itradeico.com/2018/07/smart-contracts-use-cases-and-examples-in-blockchain-simple-guide/10945

Petersen, J. (2018, October 22). IDC report describes HHS implementation of blockchain in acquisition record-keeping. Retrieved from https://www.executivegov.com/2018/10/idc-report-describes-hhs-implementation-of-blockchain-in-acquisition-record-keeping/

PolySwarm. (2018, March 7). 5 companies already brilliantly using smart contracts. Retrieved from https://medium.com/polyswarm/5-companies-already-brilliantly-using-smart-contracts-ac49f3d5c431

Radocchia, S. (2017, November 9). What are some ways blockchain smart contracts can improve government? Retrieved from https://www.quora.com/What-are-some-ways-blockchain-smart-contracts-can-improve-government

Ryan, P. (2017, October). Smart contract relations in e-commerce: Legal implications of exchanges onducted on the blockchain. Retrieved from https://timreview.ca/sites/default/files/article_PDF/Ryan_TIMReview_October2017.pdf

Schneider, T. K. (2018, July 23). HHS unveils blockchain-powered acquisition assistance. Retrieved from https://gcn.com/articles/2018/07/23/hhs-blockchain.aspx?m=1

Serbu, J. (2017, February 28). The legacy of better buying power: DoD's gambit to reform acquisition "from within." Retrieved from https://federalnewsnetwork.com/defense/2017/02/bbpndaa-special-report-part-1/

Sharma, M., Ramakrishnan, A., & Rahgozar, A. (2018, June 4). The possibilities of blockchain: Use cases for B2B, B2C and government services. Retrieved from https://tech.economictimes.indiatimes.com/news/corporate/the-possibilities-of-blockchain-use-cases-for-b2b-b2c-and-government-services/64411513

Shrier, A. A., Chang, A., Diakun-thibault, N., Forni, L., Landa, F., Mayo, J., & Van Riezen, R. (2016, August 8). Blockchain and health IT: Algorithms, privacy, and data. Retrieved from http://blocktonite.com/wp-content/uploads/2017/04/15-Winning-HHS-Papers-on-Blockchain-09.2016.pdf

Singh, P. (2018, February 2). What's the difference between blockchain and a database. Retrieved from https://www.quora.com/Whats-the-difference-between-blockchain-and-a-database

Stephenson, C. (2017, June 26). GSA calls for blockchain and machine learning to speed acquisition. Retrieved from https://www.fedscoop.com/gsa-calls-blockchain-machine-learning-speed-acquisition/

Tabora, V. (2018, August 4). Databases and blockchains, the difference is in their purpose and design. Retrieved from https://hackernoon.com/databases-and-blockchains-the-difference-is-in-their-purpose-and-design-56ba6335778b

Waedt, H. (n.d.). 10 use cases: Blockchain for the government. Retrieved from https://www.linkedin.com/pulse/10-use-cases-blockchain-government-holger-waedt/

Automatic Generation of Contractual Requirements From MBSE Artifacts

Alejandro Salado—is an Assistant Professor with the Grado Department of Industrial and Systems Engineering at Virginia Tech. His research focuses on applying decision analysis to improve the practice of engineering, in particular in the areas of verification and validation, and on improving problem formulation through modeling. Dr. Salado is a recipient of the NSF CAREER Award and the Fulbright International Science and Technology Award. He holds a BSc and an MSc in electrical engineering (Polytechnic University of Valencia), an MSc in project management and an MSc in electronics engineering (Polytechnic University of Catalonia), the SpaceTech MEng in space systems engineering (Delft University of Technology), and a PhD in systems engineering (Stevens Institute of Technology). [asalado@vt.edu]

Paul Wach—is a PhD student in Systems Engineering at Virginia Tech. His research interests include the mathematical formalism of model-based systems engineering (MBSE). Wach is currently exploring the feasibility of underpinning the Systems Modeling Language (SysML) with the mathematical Wymorian System Construct. He is also employed by the Department of Energy (DOE), where he manages $4 billion of work. While at the DOE, Wach has led implementation of enterprise- and program-level systems engineering and program management practices. He has previously worked for two of the DOE national laboratories, Pacific Northwest National Laboratory and Savannah River National Laboratory. Prior to work with the DOE labs, Wach was developing cutting edge artificial kidney technology based on his Master of Science with the University of South Carolina and medical research experience at the Medical College of Georgia. He also holds a Bachelor of Science degree in Biomedical Engineering from the Georgia Tech. [paulw86@vt.edu]

Abstract

This paper is intended to disseminate initial outcomes of the NPS Research Acquisition Program “Automatic Generation of Contractual Requirements from MBSE Artifacts” project. The research addresses the automatic generation of contractual requirements in textual form from models in a Model-Based Systems Engineering (MBSE) environment, enabling the transition from document-centric systems engineering to MBSE in acquisition programs. Textual requirements form the backbone of contracting in acquisition programs. Requirements define the problem boundaries within which contractors try to find acceptable solutions (design systems). At the same time, requirements are the criteria by which a customer measures the extent to which their contract has been fulfilled by the contractor. However, latent problems exist in acquisition programs stemming from poor practices in requirements engineering. Research suggests that transitioning to model-based requirements can be effective in coping with such challenges. We presented in prior work a framework to construct true model-based requirements within the context of the Systems Modeling Language (SysML). This research addresses the main question of whether contractual requirements in textual form can be automatically generated from those requirement models without loss of information or intent. We present in this paper an initial template of requirements and a process to support this goal.

Introduction

Textual requirements form the backbone of contracting in acquisition programs. Requirements define the problem boundaries within which contractors try to find acceptable solutions (design systems; Salado et al., 2017). At the same time, requirements are the criteria by which a customer measures the extent to which its contract has been fulfilled by the contractor (e.g., INCOSE, 2015). Hence, it is not surprising that some authors consider requirements “the cornerstone of … systems engineering” (Buede, 2009). However, literature shows latent problems in acquisition programs stemming from poor practices in requirements engineering (e.g., Yeo, 2002; Dada, 2006; McConnell, 2001; El Eman & Birk, 2000).

In order to cope with such a challenge, academia and industry envision extending the application of Model-Based Systems Engineering (MBSE) beyond conceptual design, particularly addressing problem formulation. Two main paths to integrate requirements within a complete MBSE environment are currently pursued. In the first path, major modeling languages, such as Systems Modeling Language (SysML), incorporate elements called *requirement models* (Friedenthal, Moore, & Steiner, 2015), which are intended to model the requirements the system is expected to fulfil. Some authors have attempted to demonstrate how those so-called *requirement models* can be used to move acquisition practice from document-centric (textual) requirements to model-based requirements (e.g., Holt et al., 2011; Holt et al., 2015). However, this approach is based on defining specific model elements, called "requirements," which contain a text property that takes the textual requirement. The requirement element is then linked to a specific component in the system architecture. Hence, the only modeling value of this approach is to achieve traceability between requirements and architectural elements. Although this is valuable on its own merit, requirements remain textual; thus, model-based requirements are not achieved.

In the second path, researchers propose to use behavioral models of the system of interest as problem definition elements (requirements; e.g., Miotto, 2014). Such work has been confined, though, to the technical challenges of modeling expected system behavior. Therefore, the proposition remains positional, since such work has not addressed how contracting in acquisition programs is affected, or needs to be adjusted, to incorporate behavioral models as a contractual mechanism instead of textual requirements. Hence, the near-term, practical feasibility of the approach is questionable.

In a third path, less extended, mathematical or formal structures are used to capture requirements (e.g., Micouin, 2008). In these approaches, *shall* statements or similar natural language statements are not used in the formulation of the requirement. In the context of the research presented in this paper, these representations may be considered examples of true model-based requirements. Their usage in the context of SysML is, however, not evident.

The overarching research in which this paper is framed is aimed at overcoming those obstacles by providing a translation mechanism that enables the engineering of true requirement models, while automatically generating corresponding textual requirements. Prior work by the authors has addressed the construction of such true model-based requirements in SysML (Salado & Wach, 2019). This paper presents a template and showcases a requirement translation process that enables the automatic generation of contractual requirements in natural language (i.e., textual requirements) from model-based requirements.

Background: Model-Based Requirements in SysML

The construct for model-based requirements in SysML described in Salado and Wach (2019) is used in this paper. A summary of the construction specification for such model-based requirements is provided in this section.

Justification

The key underlying construct of a model-based requirement lays upon "the central proposition … that every requirement can be modeled as an input/output transformation" executed through one or more physical interfaces (Salado & Wach, 2019). This proposition is founded on two main premises. First, every system can be modeled as a transformation of input trajectories into output trajectories (Wymore, 1993). Second, a set of requirements yields a solution space (Salado, Nilchiani, & Verma, 2017). Therefore, "it follows that a solution space can be modeled as a set of transformations of input trajectories into output trajectories" (Salado & Wach, 2019).

The suitability of this construct was explored by re-interpreting requirement categories of a taxonomy that fulfills the partition criterion as input/output transformations (Salado & Wach, 2019). Four requirement types, which are considered to be collectively exhaustive to capture requirements, were considered: functional requirements (i.e., what the system must do), performance requirements (i.e., how well the system must do it), resource requirements (i.e., what the system may consume to do those things that well), and environmental requirements (i.e., in which settings or contexts the system must do those things, that well, with those resources; Salado & Nilchiani, 2014, 2017). The explanation of how these types of requirements may be described as sets of input/output transformations provided in Salado and Wach (2019) is reproduced verbatim here:

> *Functional requirements* inherently describe input/output transformations. Mathematically, a function is necessarily defined as a mapping between a domain and codomain. From a General Systems Theory perspective, engineered systems are necessarily open (von Bertalanffy, 1969).
>
> *Performance requirements* are, as defined, necessary characteristics, properties, or attributes associated with the inputs and outputs of the transformations that the system shall perform. In fact, this condition is necessary because any attribute transparent to the interaction between the system and external systems should not be considered a requirement due to unnecessarily constraining the solution space (Salado et al., 2017, INCOSE, 2012).
>
> *Resource requirements* define limits on resources that the system may consume. It is obvious that a resource must therefore be inputted to the system and that it is consumed for producing something. Hence, any limitation imposed on resource consumption is in fact part of a functional exchange and can be modeled in such a way.
>
> *An environment for the system* is an abstraction of boundaries between the system and external systems. The environment provides certain conditions under which the system must operate and imposes certain limitations on how the system may affect the environment. In other words, the environment provides certain *inputs* under which the system must operate and imposes certain limitations on the *outputs* the system may yield to the environment.

In terms of typology of inputs and outputs, the construct is consistent with Kossiakoff et al.'s (2011) taxonomy for external interfaces and considers that systems operate in three types of media (information, material, and energy) that become inputs to and/or outputs from the system (Salado & Wach, 2019).

Construction Rules

A complete description of the construction rules for the model-based requirements is given in Salado & Wach (2019). A summary is provided here.

In line with the theoretical construct described in the previous section, the model-based requirements are built according to the meta-model depicted in Figure 1.

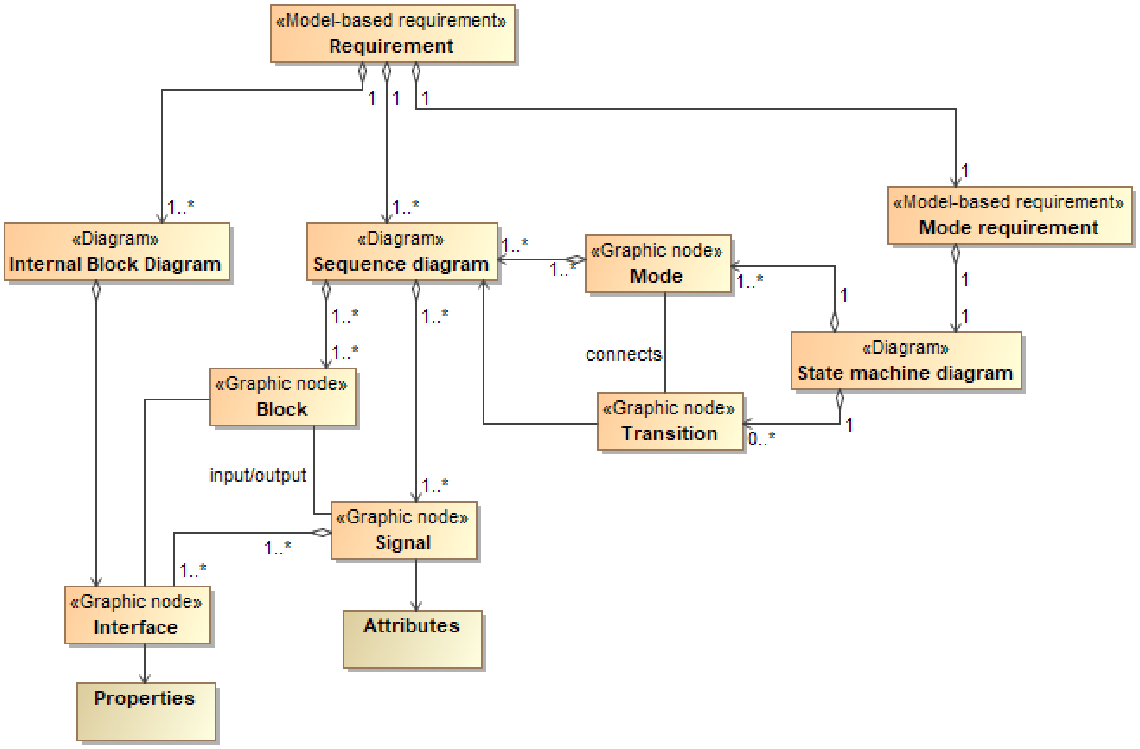


Figure 1. **Meta-Model of the Model-Based Requirements**
(Salado & Wach, 2019)

Three main SysML constructs are used to capture requirements as models (Salado & Wach, 2019):

1. A sequence diagram, which captures the required input/output exchanges. Each input or output is modeled by signal elements, which capture the required properties of each input and output. An example is provided in Figure 2.
2. An internal block diagram, which captures the physical interfaces that are required to convey the required system inputs and outputs. Each interface is modeled by ports, which capture the required properties of each interface and the signals it conveys. An example is provided in Figure 3.
3. Mode requirements, which describe the sets of requirements that apply simultaneously, modeled by state machine diagrams. Each state represents a mode, which represents a collection of requirements that need to be fulfilled simultaneously. An example is provided in Figure 4.

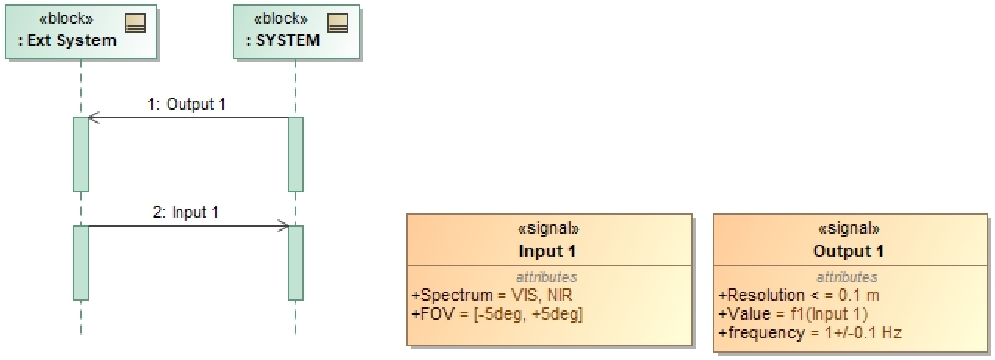


Figure 2. **Example of Input/Output Transformation As a Model-Based Requirement**
(Salado & Wach, 2019)

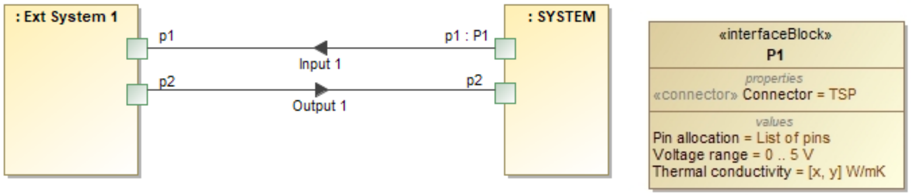


Figure 3. **Example of a Required Physical Interface Through Which the Required Input/Output Transformation Occurs as a Model-Based Requirement**
(Salado & Wach, 2019)

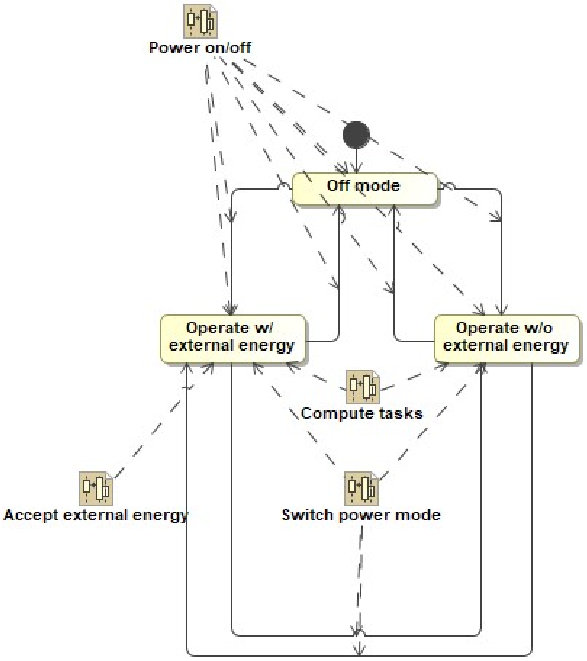


Figure 4. **Example of Requirement Sets as a Model-Based Requirement**
(Salado & Wach, 2019)

It should be noted that although existing SysML constructs are used to model requirements, there are semantic differences with respect to their regular use to model system solutions (Salado & Wach, 2019). Describing those differences is outside the scope of this paper because they are addressed in the original source. It suffices to state that the diagrams shown in this section extend (or modify in some cases) their traditional use in SysML. In essence, they should not be interpreted as models of the behavior or physical structure of the system, but as models of the input/output transformations the system is required to execute.

An Approach to Transform Model-Based Requirements to Contractual Requirements in Natural Language

Process

The process to transform the model-based requirements presented in the previous section (Background: Model-Based Requirements in SysML) to contractual requirements in natural language consists of four steps:

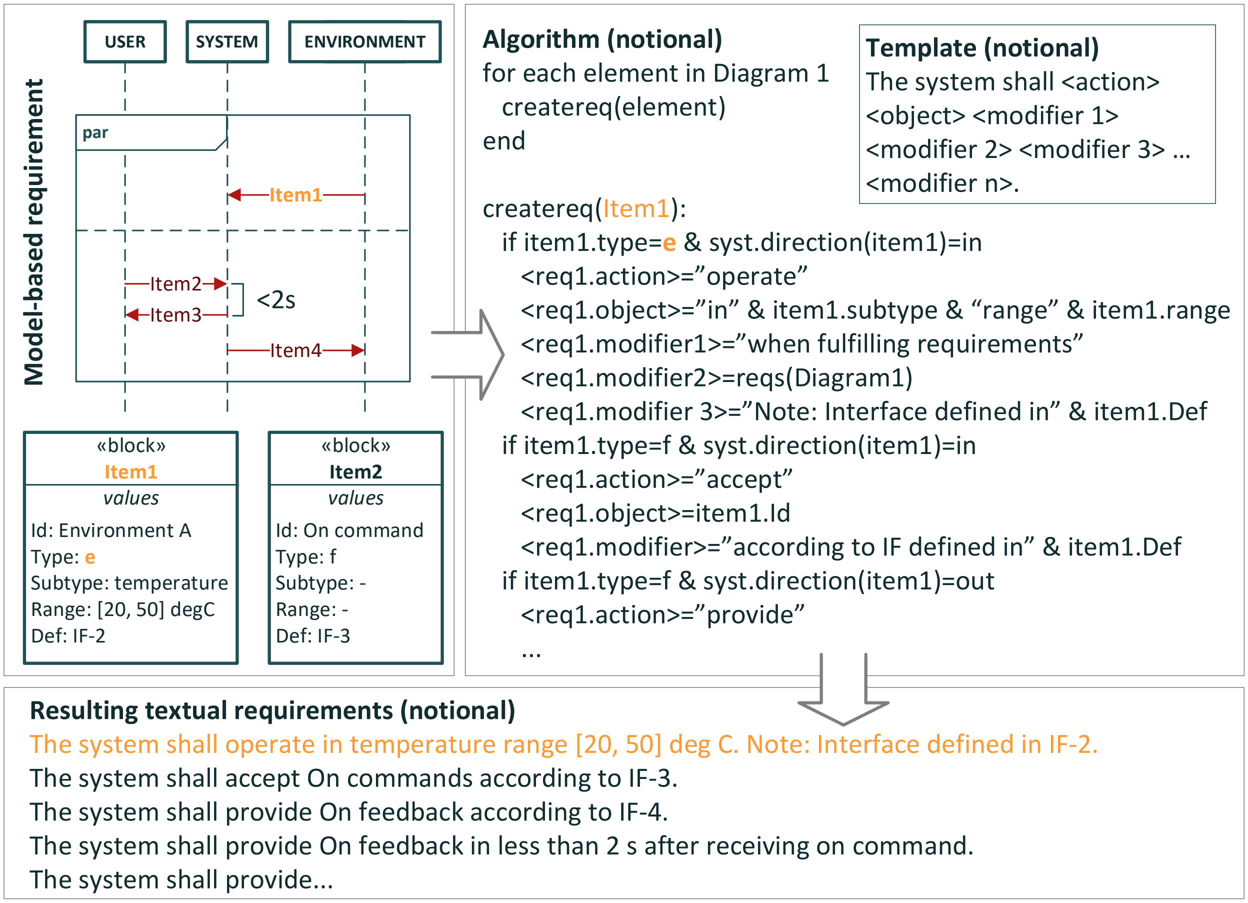
Step 1. For each port, generate corresponding textual requirements*.* This step generates a list of physical interfaces that are characterized by a set of required properties, which will be pointed at by the requirements resulting from the sequence diagrams.

Step 2. For each mode, generate a simultaneity modifier. This step assigns tags to each sequence diagram associated with a particular mode. These tags are used later to associate a modifier with the textual requirements resulting from such sequence diagrams that indicates the need to fulfill such requirements in the context of all other requirements with the same modifier.

Step 3. For each sequence diagram, generate corresponding textual requirements. This step generates a list that contains requirements associated with the need to accept inputs and provide outputs, the characteristics of those inputs and outputs, and the logical or temporal conditions for the acceptance of those inputs and provision of those outputs. In addition, for each requirement referring to the required inputs and outputs, a modifier referring to the physical interface through which such input or output is conveyed is added. Furthermore, the simultaneity modifiers in Step 2 are used to identify the subset of requirements that need to be fulfilled simultaneously.

Step 4. Remove repetitions, if any. Because inputs and outputs may be used in several sequence diagrams, this step will consolidate the list of requirements to avoid repetitions. It should be noted that this step can be executed after all textual requirements have been generated or as they are being generated, for efficiency purposes.

The basic concept for generating textual requirements leverages a predefined template of natural language requirements that maps to the different elements in the meta-model depicted in Figure 1. A simplified view of this concept is shown in Figure 5. A computerized algorithm is not used in this paper but is being developed as part of the research program. It will be disseminated in future publications. The focus of this paper lays on the template that will be employed to generate the textual requirements. Specific template rules are defined, as will be described in the next section, to cope with the different types of requirements captured by the model-based requirements.



Algorithm (notional)

```
for each element in Diagram 1
  createreq(element)
end

createreq(Item1):
  if item1.type=e & syst.direction(item1)=in
    <req1.action>=”operate”
    <req1.object>=”in” & item1.subtype & “range” & item1.range
    <req1.modifier1>=”when fulfilling requirements”
    <req1.modifier2>=reqs(Diagram1)
    <req1.modifier 3>=”Note: Interface defined in” & item1.Def
  if item1.type=f & syst.direction(item1)=in
    <req1.action>=”accept”
    <req1.object>=item1.Id
    <req1.modifier>=”according to IF defined in” & item1.Def
  if item1.type=f & syst.direction(item1)=out
    <req1.action>=”provide”
    …
```

Template (notional)
The system shall <action> <object> <modifier 1> <modifier 2> <modifier 3> … <modifier n>.

Resulting textual requirements (notional)
The system shall operate in temperature range [20, 50] deg C. Note: Interface defined in IF-2.
The system shall accept On commands according to IF-3.
The system shall provide On feedback according to IF-4.
The system shall provide On feedback in less than 2 s after receiving on command.
The system shall provide...

Figure 5. **A Representation of the Concept to Generate Textual Requirements Out of Model-Based Requirements**

Template

The basic template for a requirement takes the form of *The system shall <action> through <interface>*. This form is refined to capture the richness of requirements offered by the model-based requirements described earlier in the paper. The resulting forms are shown next.

Consider the basic model provided by the sequence diagram in Figure 2 and the internal block diagram in Figure 3. Table 1 shows the template for the requirement in natural language and describes how each element of those model-based requirements is mapped to an element of such template.

Table 1. Mapping of Model Elements to Textual Template

Template of textual requirement	Model element
The <object> shall <accept> <Input> according to <Interface>. *Note 1*: <Input> is defined in <Source 1>. *Note 2*: <Interface> is defined in <Source 2>.	<object>: Block in diagrams referred to as *System*. <accept>: Captured as an input directional port on the system in the Sequence Diagram (incoming arrow in the sequence diagram). <Input>: Name of the *Signal* connected to the input directional port in the Sequence Diagram. <Interface>: Connection between *System* block and external block in the Internal Block Diagram, to which *Signal* is allocated. This is described as a physical port in the System block. <Source 1>: Properties of the *Signal*, directly described in the properties of the element. <Source 2>: Properties of the physical interface, directly described in the properties of the *Port* element.
The <object> shall <provide> <Output> according to <Interface>. *Note 1*: <Output> is defined in <Source 1>. *Note 2*: <Interface> is defined in <Source 2>.	<object>: Block in diagrams referred to as *System*. <provide>: Captured as an output directional port on the system in the Sequence Diagram (outgoing arrow in the sequence diagram). <Output>: Name of the *Signal* connected to the output directional port in the Sequence Diagram. <Interface>: Connection between *System* block and external block in the Internal Block Diagram, to which *Signal* is allocated. This is described as a physical port in the System block. <Source 1>: Properties of the *Signal*, directly described in the properties of the element. <Source 2>: Properties of the physical interface, directly described in the properties of the *Port* element.

Consider now the model-based requirements in Figure 6, which capture required dependencies between the inputs and outputs. It should be noted that the three examples are not exhaustive, but other types of dependencies may be captured (Salado & Wach, 2019). Table 2 shows the templates for the requirement in natural language and describes how each element of model-based requirements is mapped to an element of such templates.

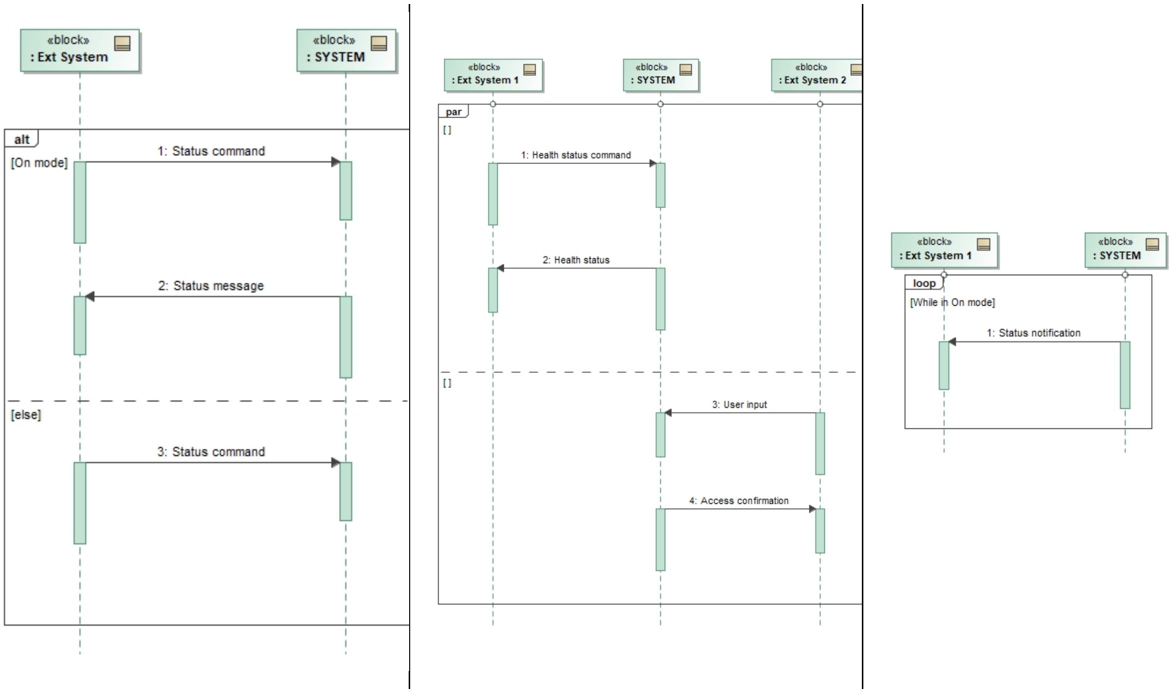


Figure 6. **Examples of Model-Based Requirements Capturing Various Dependencies Between Inputs and Outputs**

Note. Left: alternative required exchange based on conditions; Center: exchanges that need to be executed in parallel; Right: continuous exchange until a condition is met.

Table 2. Mapping of Functional Dependencies Model Elements to Textual Template

Template of textual requirement	**Model element**
The <object> shall <action> <when> in <condition>.	<object>: Block in diagrams referred to as *System*. <action>: It takes the value of *accept* or *provide* depending on whether the *Signal* element inside one of the branches of the conditional element is an input or an output, respectively to the block *System*. <when>: This value is used when the diagram element is *alt*. <condition>: As described in the condition property of the *alt* element.
The <object> shall <action 1> <while> <action 2>.	<object>: Block in diagrams referred to as *System*. <action 1>: It takes the value of *accept* or *provide* depending on whether the *Signal* element inside one of the branches of the conditional element is an input or an output, respectively to the block *System*. <while>: This value is used when the diagram element is *par*. <action 2>: It takes the value of *accept* or *provide* depending on whether the *Signal* element inside another branch of the conditional element is an input or an output, respectively to the block *System*.
The <object> shall <action> <while/for> <condition>.	<object>: Block in diagrams referred to as *System*. <action>: It takes the value of *accept* or *provide* depending on whether the *Signal* element inside the conditional element is an input or an output, respectively to the block *System*. <while/for>: This value is used when the diagram element is *loop*. <condition>: As described in the condition property of the *alt* element.

It should be noted that defining required time dependencies or restrictions between inputs and outputs may also be necessary (Salado & Wach, 2019). Figure 7 shows an example. In this case, Table 3 shows the template for the requirement in natural language and describes how each element of model-based requirements is mapped to an element of such template.

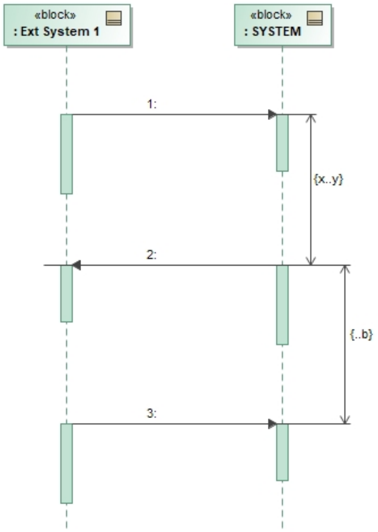


Figure 7. **Example of a Model-Based Requirement Capturing Time Restrictions**

Table 3. Mapping of Timing Dependencies Model Elements to Textual Template

Template of textual requirement	**Model element**
The <object> shall <action 1> in <time dependency> <after> <action 2>.	<object>: Block in diagrams referred to as *System*. <action 1>: It takes the value of *accept* or *provide* depending on whether the *Signal* element is an input or an output, respectively to the block *System*. <time dependency>: This is formally defined as a range of [Min, Max], which refer to dependencies such as: less than, more than, within. <after>: This is implied by the temporal dependency given by the *duration constraint*. <action 2>: It takes the value of *receiving* or *providing* depending on whether the *Signal* element is an input or an output, respectively to the block *System*.

Two options are offered for the template for capturing simultaneity of requirement applicability in natural language (as modeled for example in Figure 4). The first one is shown in Table 4, together with a description of how each element of model-based requirements is mapped to an element of such template. The second one consists in simply creating separate sections of the requirement document for each mode requirement, with a statement that reads, *All requirements in this section shall be fulfilled simultaneously*.

Table 4. Mapping of Applicability Simultaneity Model Elements to Textual Template

Template of textual requirement	Model element
<Req X>. The system shall… Note: This requirement must be fulfilled simultaneously with [<Req Y>].	<Req X> is a requirement originating from a *Sequence Diagram* linked to a *state* element. [<Req Y>] is a list of all requirements originating from all *Sequence Diagrams* linked to the *state* element to which *Sequence Diagram* from which <Req X> originates is also connected.

No template is prescribed for capturing the characteristics of inputs, outputs, and interfaces in textual form. In general, they may be listed as columns containing the property and the required values for each property. For physical interfaces, properties may be organized, for example, following a layered approach, such as identifying a transport layer and a physical layer.

Application Example

Case Design

The proposed template to transform the model-based requirements developed in this research project into natural language requirements that can be used to support contractual activities is applied to the case developed in Salado and Wach (2019). In such work, a notional set of requirements in textual form (not necessarily following any template) was transformed into a set of model-based requirements. In this paper, the resulting model-based requirements in such work are transformed back into textual requirements, but using the template presented in this paper. The resulting textual requirements are compared against those used as source requirements in the original work.

It should be noted that a formal comparison of the efficiency, coverage, and accuracy of the resulting requirements after applying the template presented in this paper is outside of the scope of this paper. The focus of the paper is to illustrate how the proposed template can be used to transform model-based requirements to textual requirements, without assessing its performance.

Problem Statement: Model-Based Requirements

The model-based requirements used in this case are depicted in Figures 8 through 15 and directly taken from Salado and Wach (2019). They represent the requirements for an optical space instrument with the purpose to take images of the Earth and send them to the satellite platform under command by the platform. In parallel, the instrument is required to provide health status data *continuously* to the satellite platform for monitoring purposes. The requirement set, which has been adapted from Salado and Nilchiani (2014) and includes new requirements that were added for coherence and partial completeness, provide nevertheless a limited set of requirements with respect to a real-life project. However, the

> acceptability and suitability of the sample requirements [were] validated by deriving and contrasting them against requirements of actual operational and scientific optical space systems developed by different manufacturers for different customers and with a similar level of complexity, which is represented by an instrument mass of around 1 ton. (Salado & Nilchiani, 2014)

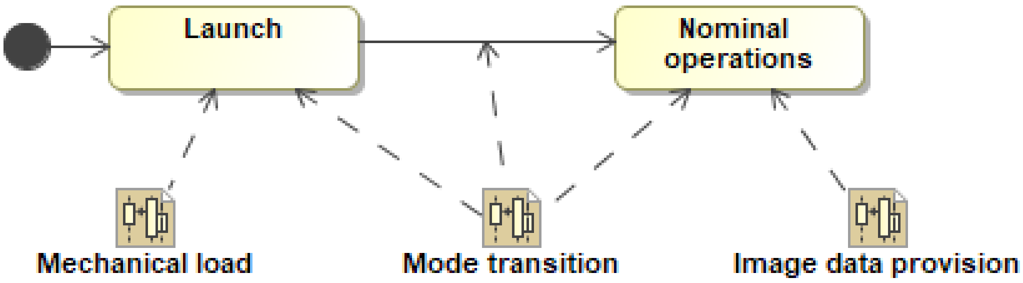


Figure 8. **Mode Requirements**
(Salado & Wach, 2019)

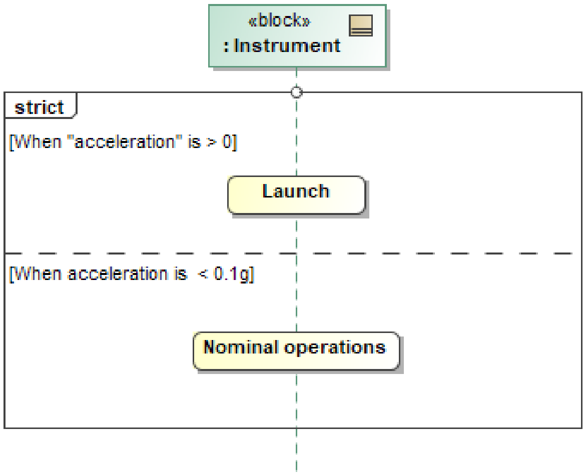


Figure 9. **Conditions for Applicability of Each Subset of Requirements (Mode Transition in Figure 8)**
(Salado & Wach, 2019)

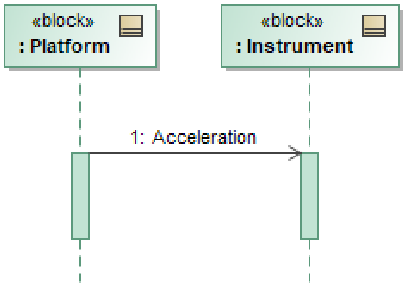
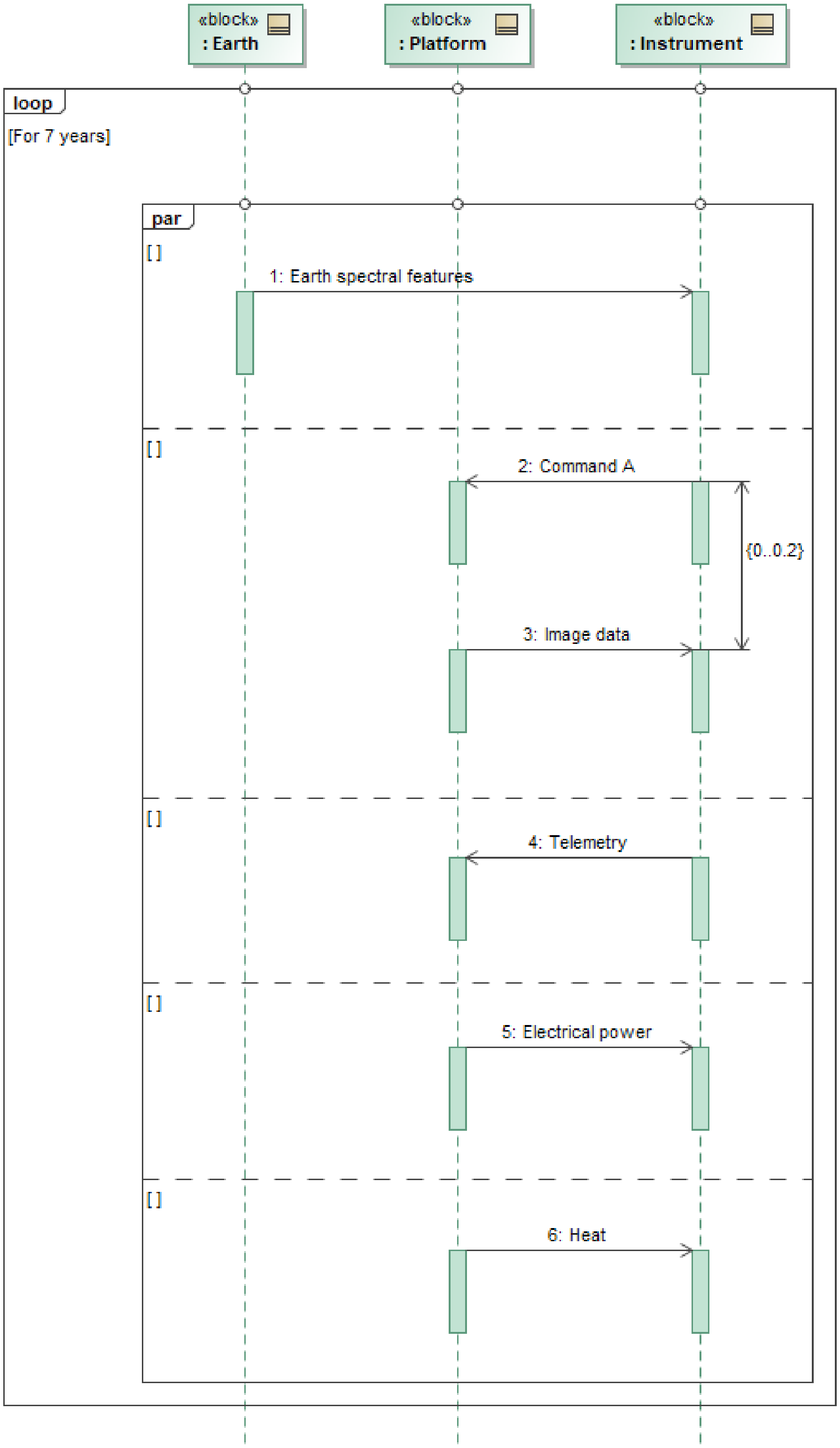


Figure 10. **Exchange Related to the Mechanical Load Requirement**
(Salado & Wach, 2019)



Note. There is an error in the figure: Command A is an input to the Instrument, and Image data is an output of the Instrument.

Figure 11. **Required Exchanges in Nominal Operations**
(Salado & Wach, 2019)

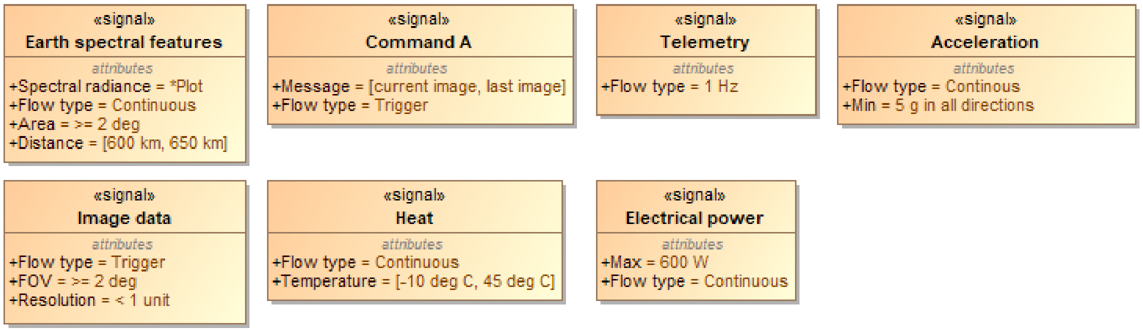


Figure 12. **Required Characteristics of the Required Inputs and Outputs**
(Salado & Wach, 2019)

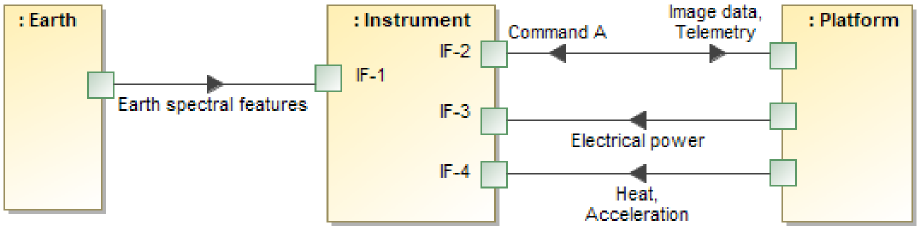


Figure 13. **Requirements on the Allocation of Logical Inputs and Outputs to Physical Interfaces Through Which They Must Be Conveyed**
(Salado & Wach, 2019)

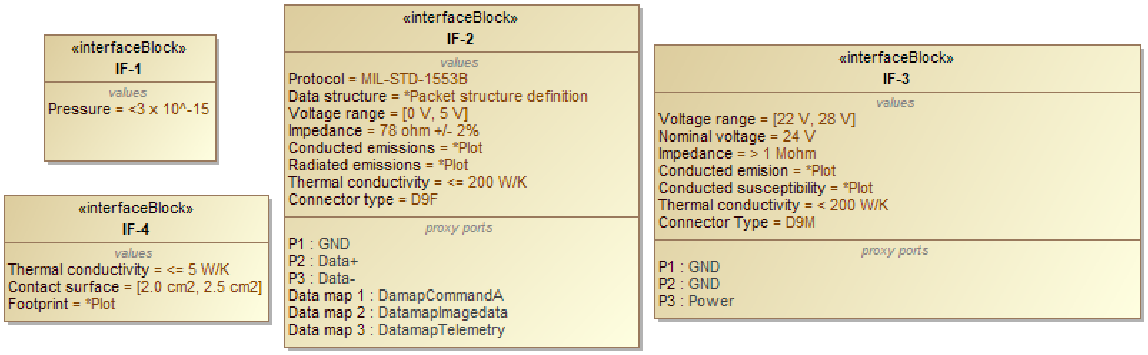

«interfaceBlock»
IF-1
values
Pressure = <3 x 10^-15
«interfaceBlock»
IF-4
values
Thermal conductivity = <= 5 W/K
Contact surface = [2.0 cm2, 2.5 cm2]
Footprint = *Plot
«interfaceBlock»
IF-2
values
Protocol = MIL-STD-1553B
Data structure = *Packet structure definition
Voltage range = [0 V, 5 V]
Impedance = 78 ohm +/- 2%
Conducted emissions = *Plot
Radiated emissions = *Plot
Thermal conductivity = <= 200 W/K
Connector type = D9F
proxy ports
P1 : GND
P2 : Data+
P3 : Data-
Data map 1 : DamapCommandA
Data map 2 : DatamapImagedata
Data map 3 : DatamapTelemetry
«interfaceBlock»
IF-3
values
Voltage range = [22 V, 28 V]
Nominal voltage = 24 V
Impedance = > 1 Mohm
Conducted emision = *Plot
Conducted susceptibility = *Plot
Thermal conductivity = < 200 W/K
Connector Type = D9M
proxy ports
P1 : GND
P2 : GND
P3 : Power

Figure 14. **Required Characteristics of the Physical Interfaces Through Which Inputs and Outputs Must Be Conveyed**
(Salado & Wach, 2019)

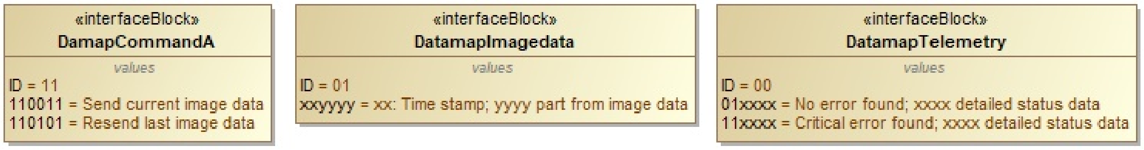

«interfaceBlock»
DamapCommandA
values
ID = 11
110011 = Send current image data
110101 = Resend last image data
«interfaceBlock»
DatamapImagedata
values
ID = 01
xxyyyyy = xx: Time stamp; yyyy part from image data
«interfaceBlock»
DatamapTelemetry
values
ID = 00
01xxxx = No error found; xxxx detailed status data
11xxxx = Critical error found; xxxx detailed status data

Figure 15. **Modeling of Transport Layer Aspects as Proxy Ports for Leveraging Model Complexity**
(Salado & Wach, 2019)

Resulting Contractual Requirements in Natural Language

Application of Step 1. Each interface block in Figure 14 is converted to a table form with two columns, one listing the property and one listing the corresponding value. It should be noted that, as part of those properties, the information in Figure 15 is nested for some of the interfaces in Figure 14**.** The resulting tables are not shown in this paper because of length limitations. For referencing purposes in other requirements, they will be referred to as Tables E1 through E4, which correspond to IF-1 through IF-4, respectively.

Application of Step 2. For simplicity, the approach to divide the requirement set in sections is used. Two sections are therefore created. Section 1 corresponds to *Launch* requirements, and Section 2 corresponds to *Nominal Operations* requirements.

Application of Step 3. First, all signals in Figure 12 are converted to a table form with two columns, one listing the property and one listing the corresponding value (ref. Table 5). A template in Table 1 is applied to Figures 10 and 13, yielding a single requirement for the *Launch* requirements subset. All templates are then used on Figures 11 and 13 to generate the requirements for the *Nominal Operations* subset. The resulting requirements are given in Table 6. Requirements R2 through R7 are generated using template in Table 1. Requirement R8 is generated using templates in Table 3. Requirements R9 and R10 are generated using templates in Table 2. Note that R9 and R10 have been simplified because of paper length limitations. Essentially, the requirements should be extended to every action that is paralleled and every action that is part of the lifetime loop, respectively.

Table 5. Required Characteristics of Inputs and Outputs

Property	**Value**
S1	
Flow type	Continuous
Min	5g in all directions
S2	
Spectral radiance	*Plot
Flow type	Continuous
Area	>= 2 deg
Distance	[600 km, 650 km]
S3	
Message	[current image, last image]
Flow type	Trigger
S4	
Flow type	Continuous
Temperature	[-10 deg C, 45 deg C]
S5	
Max	600 W
Flow type	Continuous
S6	
Flow type	Trigger
Field of View	>= 2 deg
Resolution	< 1 unit
S7	
Flow type	1 Hz

Table 6. Resulting Textual Requirements

ID	Requirement
Launch Note: All requirements in this section must be fulfilled simultaneously.	
R1	The system shall accept Acceleration according to IF-4. Note 1: Acceleration is defined in Table S1. Note 2: IF-4 is defined in Table E4.
Nominal Operations Note: All requirements in this section must be fulfilled simultaneously.	
R2	The system shall accept Earth spectral features according to IF-1. Note 1: Earth spectral features are defined in Table S2. Note 2: IF-1 is defined in Table E1.
R3	The system shall accept Command A according to IF-2. Note 1: Earth spectral features are defined in Table S3. Note 2: IF-2 is defined in Table E2.
R4	The system shall accept Electrical power according to IF-3. Note 1: Earth spectral features are defined in Table S4. Note 2: IF-3 is defined in Table E3.
R5	The system shall accept Heat according to IF-4. Note 1: Earth spectral features are defined in Table S5. Note 2: IF-4 is defined in Table E4.
R6	The system shall provide Image data according to IF-2. Note 1: Earth spectral features are defined in Table S6. Note 2: IF-2 is defined in Table E2.
R7	The system shall accept Telemetry according to IF-2. Note 1: Earth spectral features are defined in Table S7. Note 2: IF-2 is defined in Table E2.
R8	The system shall provide Image data in less than 0.2 s after having received Command A.
R9	The system shall accept Earth spectral features while accepting [Command A, Electrical Power, Heat] and providing [Image data, Telemetry].
R10	The system shall <all actions> for 7 years.

Step 4 has not been applied in this example.

Comparison and Discussion

The resulting textual requirements for the required properties of the physical interfaces captured in Figures 14 and 15 are identical to those in the benchmark given in Salado and Wach (2019), although they have not been explicitly shown in this paper. However, a comparison of the description of the resulting requirements in table form with those tables in the source paper yield this conclusion.

With respect to requirements in Tables 5 and 6, it is necessary to look at the benchmark textual requirements, which are listed in Table 7 directly from the original source in Salado and Wach (2019). The requirement sets look different at first sight and, in fact, present also some differences with respect to the solution space. They are discussed next.

Table 7. Benchmark Textual Requirements

(Adapted from Salado & Wach, 2019)

Req ID	Description
BR1	The instrument shall image a target at 600 km–650 km according to IF-1.
BR2	The instrument shall image a target with spectral radiance of ABC (*plot) according to IF-1.
BR3	The instrument shall accept Command A according to IF-2.
BR4	The instrument shall transmit image data according to IF-2 in less than 0.2 s after receiving Command A.
BR5	The instrument shall have a resolution better than 1 unit.
BR6	The instrument shall have a FOV greater than 2°.
BR7	The instrument shall provide telemetry data every 1 s according to IF-2.
BR8	The instrument shall accept power according to IF-3.
BR9	The instrument shall consume less than 600 W of electrical power.
BR10	The instrument shall withstand a mechanical load of 5 g in any direction on IF-4.
BR11	The instrument shall fulfill its performance when subjected to a temperature between -10 deg C and +45 deg C at IF-4.
BR12	The instrument shall have a lifetime of at least 7 years.
Note 1	R10 only applies during launch. All other requirements only apply once the instrument is powered on through IF-3.

In terms of visual differences, a different approach is taken for describing the different modes. However, this is purely a stylistic matter and of no real concern for the definition of the solution space. In addition, the benchmark employed a single requirement for each required property of the required system inputs and outputs, whereas the resulting set in this paper employs a table form for the properties linked to a single requirement for each input and output. We believe that both options have pros and cons with respect to requirement management. For example, the benchmark option may be easier to manage in terms of traceability in requirements management tools. However, it does not present any structure to facilitate consistency during requirement elicitation. Certainly, there may be ways to overcome both problems with both approaches. Hence, these differences remain aesthetic and with no impact on the definition of the solution space. Therefore, they can be considered equivalent.

Wording employed in the textual statements is also different. The free form employed in the benchmark yields the use of verbs that provide a description of the intent or purpose expected to be fulfilled by the system, whereas the proposed template uses only accepting/providing statements. We argue that the proposed approach is actually more effective. We base this assertion on two aspects. First, the purpose of deriving stakeholder needs into system requirements is to devoid the requirements of context, so that only what the system has to do is defined, not what an external actor will do with the actions of the system. In this sense, and using systems theory, a system can be fully characterized by the inputs it accepts from the environment and external systems and the output it provides to them. Second, natural language lends itself towards diversity of interpretation. This difference can cause a difference in the content of the solution space, as different engineers work towards finding an acceptable solution. Therefore, limiting the types of actions that the system can take, as proposed in this paper, may be beneficial to cope with such limitation of natural language.

In terms of effects on the solution space beyond wording interpretation, the only apparent difference is that the benchmark did not explicitly refer to the need to execute certain actions in parallel, while the models did. We believe that this difference is just an artifact of the limitations of the case study but felt it was necessary to mention for completeness. Therefore, we consider both sets of requirements to be equivalent from this perspective.

Finally, it should be noted that the transition requirements captured in Figure 9 have not been transformed to textual requirements. The reason is that the model-based requirements were incomplete and did not capture the external conditions for the different mode requirements as external inputs (particularly, pressure conditions), but just as operational conditions of the transitions. Because of this lack of completeness, the templates cannot be applied in this case.

Conclusions

Prior work in the frame of this research project demonstrated an approach to capture requirements directly in model-based form without using requirements in natural language, such as the traditional *shall* requirement statements. This paper has shown a template to generate contractual requirements in natural language directly out of those model-based requirements. These templates can enable a technical team to transition to model-based requirements while guaranteeing fulfillment of the expectation of contractual departments and acquisition programs. The former can work directly in developing models, while the latter can still provide *shall* statements to vendors and suppliers.

It should be noted that the effort is ongoing and is planned to be completed within the timeframe of the NPS Research Acquisition Program's "Automatic Generation of Contractual Requirements from MBSE Artifacts" project.

References

Buede, D. M. (2009). *The engineering design of systems: Models and methods*. Wiley.

Dada, D. (2006). The failure of e-government in developing countries: A literature review. *Electroninc Journal of Information Systems in Developing Countries, 26*, 1–10.

El Eman, K., & Birk, A. (2000). Validating the ISO/IEC 15504 measure of software requirements analysis process capability. *IEEE Transactions in Software Engineering, 26*, 541566.

Friedenthal, S., Moore, A., & Steiner, R. (2015). *A practical guide to SysML—The systems modeling language.* Waltham, MA: Morgan Kaufman.

Holt, J., Perry, S., Payne, R., Bryans, J., Hallerstede, S., & Hansen, F. O. (2015). A model-based approach for requirements engineering for systems of systems. *IEEE Systems Journal, 9*, 252–262.

Holt, J., Perry, S. A., & Brownsword, M. (2011). *Model-based requirements engineering*. IET.

INCOSE. (2012). *Guide for writing requirements*. The International Council of Systems Engineering.

INCOSE. (2015). *Systems engineering handbook: A guide for system life cycle processes and activities.* Hoboken, NJ: John Wiley and Sons.

Kossiakoff, A., Sweet, W. N., Seymour, S. J., & Biemer, S. M. (2011). *Systems engineering principles and practice.* Hoboken, NJ: John Wiley & Sons.

McConnell, S. (2001). From the editor—An ounce of prevention. *IEEE Software, 18*, 5–7.

Micouin, P. (2008). Toward a property based requirements theory: System requirements structured as a semilattice. *Systems Engineering, 11*(3).

Miotto, B. L. A. P. (2014). Model-based requirement generation. 2014 IEEE Aerospace Conference, Big Sky, MT.

Salado, A., & Nilchiani, R. (2014). A categorization model of requirements based on Max-Neef's model of human needs. *Systems Engineering, 17*, 348–360.

Salado, A., & Nilchiani, R. (2017). Reducing excess requirements through orthogonal categorizations during problem formulation: Results of a factorial experiment. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 47*, 405–415.

Salado, A., Nilchiani, R., & Verma, D. (2017). A contribution to the scientific foundations of systems engineering: Solution spaces and requirements. *Journal of Systems Science and Systems Engineering, 26*, 549–589.

Salado, A., & Wach, P. (2019). Constructing true model-based requirements in SysML. *Systems, 7*, 19.

Von Bertalanffy, L. (1969). *General systems theory—Foundations, development, applications.* New York, NY: George Braziller.

Wymore, A. W. (1993). *Model-based systems engineering.* Boca Raton, FL: CRC Press.

Yeo, K. T. (2002). Critical failure factors in information system projects. *International Journal of Project Management, 20*, 241–246.

Acknowledgements & Disclaimer

This material is based upon work supported by the Acquisition Research Program under HQ0034-18-1-0006. The views expressed in written materials or publications, and/or made by speakers, moderators, and presenters, do not necessarily reflect the official policies of the Department of Defense nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Computing Without Revealing: A Cryptographic Approach to eProcurement

Siva C Chaduvula—is a PhD student at Purdue University. His research interests are in cryptography, machine learning, and design. Prior to his PhD, he worked as a Deputy Manager at Bosch Limited. He completed his bachelor's and master's from Indian Institute of Technology Madras (IITM), Chennai, India.

Jitesh H. Panchal—is an Associate Professor in the School of Mechanical Engineering at Purdue University. He received his BTech (2000) from Indian Institute of Technology (IIT) Guwahati, and MS (2003) and PhD (2005) in mechanical engineering from Georgia Institute of Technology. Panchal's research interests are in the science of systems engineering with focus on three areas: democratization of design and manufacturing, decision making in decentralized socio-technical systems, and integrated products and materials design. He is a co-author of the book *Integrated Design of Multiscale, Multifunctional Materials and Products*. He is a recipient of the CAREER award from the National Science Foundation (NSF), the Young Engineer Award and two best paper awards from ASME CIE division, and a university silver medal from IIT Guwahati.

Mikhail J. Atallah—has research interests in information security and algorithms. His work on key management received the 2015 CCS Test of Time Award. He was the 2017 recipient of the Purdue Arden L. Bement, Jr. Award, the most prestigious award the university bestows in pure and applied science and engineering. He was the 2016 recipient of the Purdue Sigma Xi Faculty Research Award and the 2013 recipient of the Purdue Outstanding Commercialization Award. He is a Fellow of both the ACM and IEEE, and was a speaker nine times in the Distinguished Lecture Series of top computer science departments. Atallah has been the keynote and invited speaker at many national and international meetings and has served on the editorial boards of top journals and on the program committees of top conferences and workshops. He was selected in 1999 as one of the best teachers in the history of Purdue University and included in Purdue's Book of Great Teachers, a permanent wall display of Purdue's best teachers past and present. In 2001, he co-founded Arxan Technologies Inc to commercialize a software protection technology developed jointly with his doctoral student Hoi Chang. (In October 2015, Arxan reported that applications secured by it were running on more than 500 million devices.) He was CTO of Arxan Technologies and Chief Scientist for its defense subsidiary, Arxan Defense Systems. Arxan Defense Systems was acquired in 2010 by Microsemi Corporation, and Arxan Technologies was acquired in 2013 by the private equity firm TA Associates.

Abstract

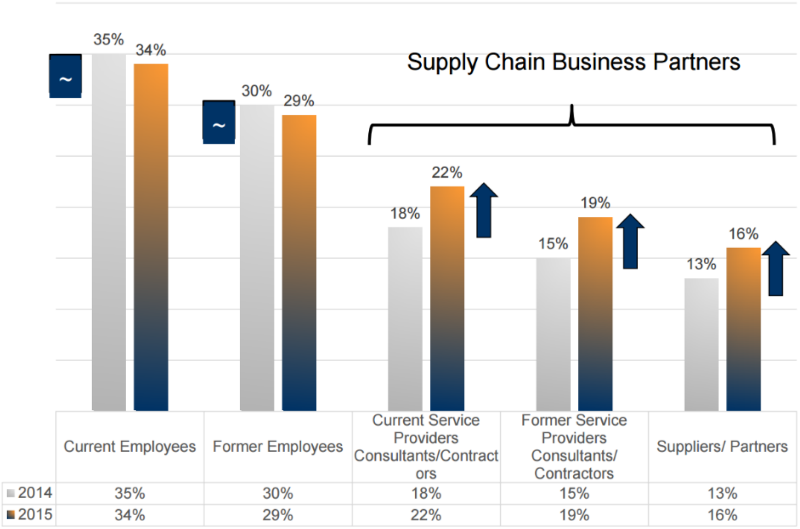
In typical eProcurement processes, sensitive data such as prices, intellectual property, and customer information often flow across enterprise boundaries. Such data sharing amplifies the risk of a data breach due to exposure to the potential security flaws of prospective and current eProcurement partners. Threats of information leakage inhibit enterprises from sharing sensitive data; thus, enterprises cannot take full advantage of the eProcurement process. Existing cryptography-based data sharing protocols impose a high computational burden for maintaining data confidentiality, making them unsuitable for real-time applications such as eProcurement. With this motivation, we address the following research question: How can procurers and suppliers securely conduct their business transactions without revealing their confidential information?

The proposed approach enables procurers and suppliers to perform computations while preserving their confidential data. In this paper, we show how Computing-Without-Revealing (CWR)–based data sharing protocols can be used as building blocks to execute procurement auctions for standard products. A web-based platform is developed to measure the performance of the CWR protocols against competing techniques. Experimental results corroborate the efficiency of the CWR-based protocols, making them suitable for real-time

applications. The application of the protocols is demonstrated for different eProcurement scenarios, including first- and second-price auctions for standard products.

Introduction

The design and manufacturing of products, regardless of complexity, involve partnerships with third-party vendors, manufacturers, suppliers, contractors, and other entities outside the organization. The design of a Boeing 777 airplane, for example, involved more than 10,000 people external to Boeing. Similarly, Ford Motor Company works with more than 1,000 suppliers across the globe. Such partnerships allow organizations to focus on their core expertise, thereby increasing their effectiveness. However, there are also risks associated with sharing confidential information with business partners. In the 2016 acquisition research symposium, it was highlighted that business partners pose a significant malicious threat because they are a part of the information flow (see Figure 1). Therefore, there is a growing need for research and development on technologies that enable business transactions without revealing confidential information of the participants.



	Current Employees	Former Employees	Current Service Providers Consultants/Contractors	Former Service Providers Consultants/ Contractors	Suppliers/ Partners
▪ 2014	35%	30%	18%	15%	13%
▪ 2015	34%	29%	22%	19%	16%

* Adapted from the PwC *The Global State of Information Security® Survey 2016,*

Figure 1. **Incidents of Data Breaches Among Business Partners**
(Kaestner, Arndt, & Dillon-Merrill, 2016)

Traditionally, business transactions between a procurer and suppliers involve a trusted third party (TTP), such as a cloud service provider. The procurer and suppliers send their confidential information to a TTP, who performs the required computation. Although this is easy to implement, the main risk is that rogue employees of the TTP (e.g., the people who maintain and update cloud servers) can learn the confidential information. Additionally, information may be compromised through a break-in by hackers, through a malware or spyware infestation, or even in a completely non-malicious (i.e., accidental) manner. There is also a potential risk that the cloud service provider may, as an organization, decide to betray the users by revealing or secretly using their confidential inputs. A recent report (Ponemon, 2018) highlighted the impact of internal attacks by insiders/contractors on organizations (see Figure 2). Therefore, it is important to preserve the confidentiality of an organization's data while engaging with current and especially potential suppliers.

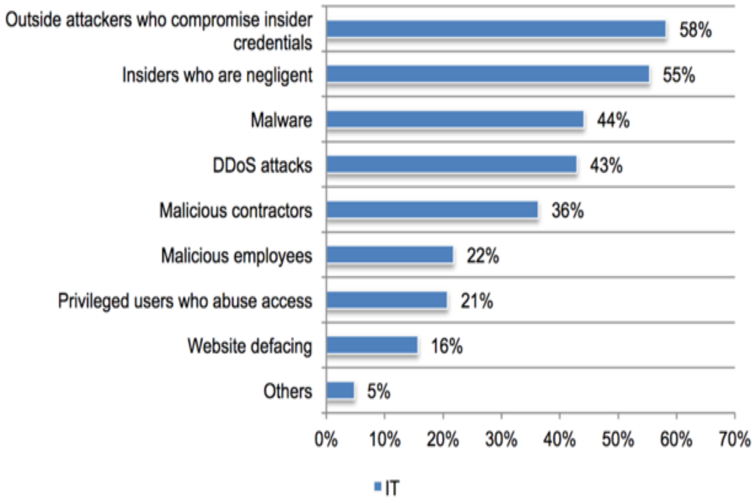


Figure 2. **Influence of Different Security Threats Faced by Organizations** (Ponemon, 2018)

In a typical eProcurement process, sensitive information related to prices, intellectual property, and customer data often flow across enterprise boundaries. While this data flow between eProcurement partners is important for performing business operations, there exist data security concerns, especially when the data involves intellectual property, trade secrets, etc. Sharing such confidential data amplifies the risk of data breach due to potential security flaws of the partners in the eProcurement process. Such threats discourage enterprises from sharing sensitive data, and thus prevents them from taking full advantage of the eProcurement process.

In this paper, we present an approach for addressing this fundamental challenge. The approach enables secure eProcurement of standard products. We present the use of cryptographic protocols to execute auction mechanisms within an eProcurement process, where the procurer only learns confidential information related to winning bidders. No confidential information about the losing bidders is revealed to anyone, including the procurer, thereby resulting in truthful revelation and increasing value for all participants involved. This proposed eProcurement process promises economic advantages for a wide variety of private-sector organizations ranging from large electronics manufacturers and automakers to small and medium-sized enterprises specializing in specific technologies.

Overview of the Approach

Current procurement processes are characterized by incomplete and disaggregated information about (i) the capabilities and cost structure of individual suppliers and (ii) the requirements of the procurers. In a typical eProcurement process, such as a sealed-bid reverse auction, as shown in Figure 3, procurement happens in three stages. In Stage 1, the procurer reveals his/her requirements to the suppliers. In Stage 2, suppliers submit their consolidated bids. In Stage 3, the procurer analyzes the submissions and determines the winner by choosing the supplier with the best technology at the lowest bidding price.

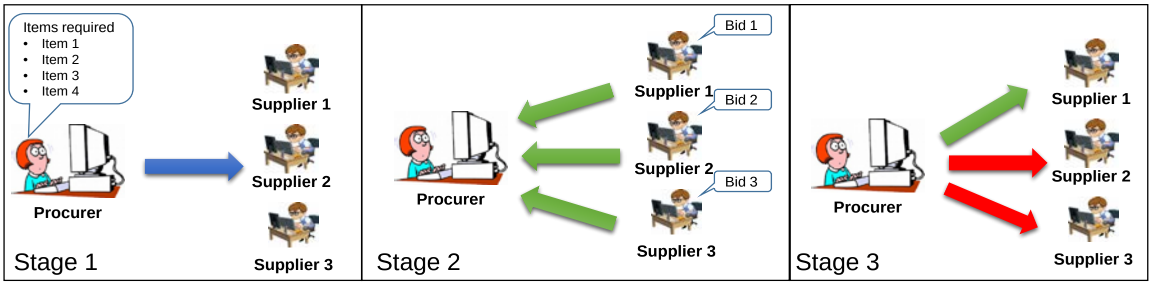


Figure 3. **Existing Approach for Sealed-Bid Auctions**

In such a setting, suppliers would ideally like the procurer to learn their confidential cost information and the details of the proprietary technology only if they win the contract. However, procurers need to determine the quality and suitability of the technology to choose the winner. In addition, procurers may not want to reveal their requirements, especially if the requirements reveal their competitive advantage. This reluctance to reveal sensitive information may drive the procurer to settle for inferior solutions, thereby reducing the overall effectiveness of the procurement mechanism. This brings us to the research question addressed in this study: How can procurers and suppliers securely conduct their business transactions without revealing their confidential information?

Our central hypothesis for this project is that the fundamental protocols discussed in the Details of the Technical Approach section can be used as building blocks to perform the computations involved in an eProcurement process. Computational results derived using Computing-Without-Revealing (CWR) protocols help in reducing information asymmetry while also protecting the sensitive information held by procurers and suppliers. Such an approach enables procurers and suppliers to estimate the challenges and uncertainties involved and thereby help both sides of the eProcurement process in making informed decisions.

Procurement processes based on the proposed CWR approach enjoy the following benefits:

- **No cryptographic key management:** No data is lost if the secret key used for determining the splits is inadvertently lost.
- **Computation time:** The proposed protocols are computationally lightweight, unlike homomorphic encryption and circuit evaluation. Hence, it is possible to perform huge computations with weaker and battery-powered portable devices such as smart phones.
- **No data abuse:** The data is handled by cloud servers, procurers, and suppliers. No user learns the actual inputs of their counterparts. Hence, there is no possibility of misusing the data. Even if there is a breach in one of the cloud servers, the data that a hacker can access would only be a share of the actual data.
- **No specialized infrastructure required:** Since their confidential information is protected, procurers and suppliers can use commercial cloud services for procurement processes. This has cost advantages in terms of capital expenditure and IT expenses.
- **Overcomes supplier vulnerabilities:** The procurer need not worry about a data breach at the supplier’s end as the data breached (if any) at the vendor’s end will

be only a share of the actual data. Therefore, no meaningful data would be leaked.

A sub-field within cryptography, called "secure multi-party computations" (SMC), focuses on enabling multiple parties to jointly process their individual confidential data into useful information while preserving the confidentiality of the data belonging to each party. Existing cryptographic practices to perform computations securely can be classified into two broad categories:

1. **No Need of a Third Party:** Cryptographic techniques such as fully homomorphic encryption (Bogetoft et al., 2009), secure circuit evaluation [Ben-David, Nisan, & Pinkas, 2008), and partial homomorphic encryption (PHE; Paillier, 1999) use encryption-based techniques to hide confidential data. Encrypted data is exchanged between parties and computations are performed on the exchanged encrypted data. Such computations impose a very high computational burden and the times reported using these techniques are much longer than in the case of the traditional TTP approach, which makes them ill-suited for use in practical scenarios.
2. **No Need to Reveal to the Third Party:** On the other hand, using secret sharing techniques is a way to distribute a secret (or confidential data) among a group of parties, where every party is allocated a share of the secret. This secret can be reconstructed only when a sufficient number of shares are combined. Individual shares do not infer anything about the whole secret.

Secret sharing approaches are comparatively faster than encryption-based approaches. The approach proposed in this study reduces the computational burden, which makes it easier to adapt. Moreover, as the proposed approach is based on general arithmetic primitives, it is well suited for quickly building secure collaborative computing platforms for new procurement scenarios or for variants of the current state of practice, such as volume-based pricing, which is not handled in previous work.

Details of the Technical Approach

EProcurement involves standard processes such as request for proposals (RFPs), auctions, payments, etc. Usually, these processes require inputs from both procurers and suppliers. We present a secure multi-party computation (SMC) technique that allows procurers and suppliers to perform the computations involved in these standard processes without needing to reveal their confidential inputs to anyone. We term our approach of the SMC technique as Computing-Without-Revealing (CWR). It builds on the protocols developed by the PIs, which are presented in Wang et al. (2017). The approach is based on two key principles (Wang et al., 2013):

- Adding/multiplying an input with a random number hides the value of the input. If the random number is much larger than the input, it also hides the order of magnitude.
- Adding/multiplying with a large number is orders of magnitude faster than the use of expensive cryptographic techniques such as homomorphic encryption and secure circuit evaluation.

Consider a scenario where the confidential value is 11. We additively split the value into random-looking shares and a participating cloud server sees only one of the random-looking shares. For example, the additive splits of 11 could be 1819 and –1808 (see Figure 4); it could just as well have been 103 and –92 or –19 and 30. These additively split values of 11 are stored in two different cloud servers. We developed protocols for basic arithmetic operations on such additive splits (see Wang et al., 2017, for details).

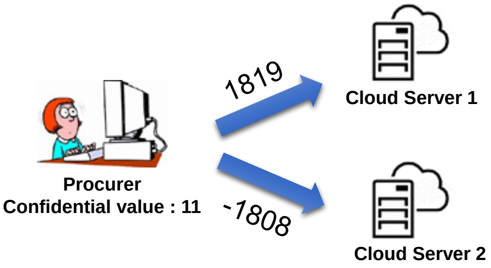


Figure 4. **Additive Splits**

The CWR approach utilizes these splits to perform the desired computation without revealing the input data to anyone. In the next section, we review the structure of the CWR protocols.

Foundational Computing-Without-Revealing (CWR) Protocols

CWR protocols enable a procurer (referred to as Alice) and suppliers (referred to as Bob) to use a single external server (referred to as Helper) to perform the computations that are mutually agreed upon between Alice and Bob. The following is the generalized structure of the CWR protocols:

- **Stage 1—Pre-processing of inputs.** The pre-processing of inputs involves two steps:

  (a) Split the inputs additively if the inputs from Alice/Bob are not additive splits.

  (b) Alice/Bob agree on a morphing function and a distribution from which random numbers are generated. Alice/Bob morph the additive splits using this morphing function and random numbers from the distribution. These morphed additive splits prevent the Helper from learning about Alice/Bob when shared with the Helper.

- **Stage 2—Run the desired computations securely.** Alice/Bob derive the application logic from their mutually agreed computation. Alice/Bob provide the application logic along with the morphed additive splits to the Helper. The application logic involves the sequence of computations that need to be performed on the morphed additive splits. The output derived from running the application logic is additively split. One of the additive splits corresponding to the output is shared with Alice and the other with Bob.

- **Stage 3—Post processing of outputs.** Alice and Bob post-process their additive splits before sharing them with each other. Alice and Bob simultaneously exchange the processed outputs with each other. Alice and Bob independently add their additive splits and learn the actual output of the computation.

Using this structure, CWR protocols for fundamental mathematical operations are proposed (Wang et al., 2017). In the rest of this paper, we denote CWR-MP to denote multiplication protocol and CWR-GT0 to denote greater than zero protocol within the CWR setting. These foundational protocols are used as building blocks to construct protocols for higher level mathematical calculations. In the next section, we discuss how these protocols can be extended to eProcurement.

Extension of CWR to eProcurement

In this paper, we present a procurement platform that enables participants of a procurement process to execute the computations involved using CWR technology. Specifically, we focused on an auction platform for standard products. However, this approach can be extended to different types of auctions suited for their business needs.

In the following sections, we describe these CWR-based auction platforms in a greater detail.

Extension of CWR to Auctions for Standard Products

In this section, we assume that standard products or commercial-off-the-shelf items are those items where the quality of these products is established. So, the decision on the auction winner is based on the price of the product.

While there are many ways to perform auctions within an eProcurement process for standard products, in what follows, we use reverse sealed-bid auctions to illustrate how CWR protocols can be used as building blocks to perform the computations involved (as shown in Figure 4). Note that the CWR-protocols can be constructed to perform the computations involved in any auction mechanism, but to simplify the discussion, we focus on the first price reverse sealed-bid auction. The computation involved in such auctions is the identification of a supplier with the minimum consolidated bid for all the items listed by the procurer. The procurer and suppliers mutually agree on three external servers (for example, cloud servers $\alpha, \beta, \text{and } \gamma$). The procurer provides unique IDs to all the suppliers. Suppliers share the additive splits corresponding to their confidential information (i.e., consolidated bids) along with their IDs with cloud server α and cloud server β. Cloud server α (as Alice) and cloud server β (as Bob), together with cloud server γ (as Helper), deploy Protocol 1. After Protocol 1 ends, the cloud servers $\alpha \text{ and } \beta$ share the additive splits obtained with the procurer. By adding these additive splits, the procurer finds the supplier with the minimum consolidated bid and the value of the consolidated bid.

This extension of CWR to eProcurement enables procurers and suppliers to perform procurement transactions without needing to reveal their confidential information to anyone. This allows procurers to design auction mechanisms that can help them overcome inefficiencies in existing auction mechanisms. For example, an auction mechanism built using CWR can identify the supplier with the best price (i.e., “cherry pick” the suppliers) for each and every item. Such an auction mechanism has great potential to reduce procurement costs, as the procurer gets the best possible price for every item. This will appeal to suppliers as well because their individual item prices are not revealed to anyone, including to the procurer. In this section, we present a CWR first price reverse auction that enables the procurer to select the supplier who provides the greatest bang for their buck for each individual item and thereby overcome this inefficiency.

CWR First Price Reverse Auction

In a CWR first price reverse auction, a single procurer (say, the DoD) can “cherry pick” the best supplier among the suppliers (DoD contractors) for each and every item. Figure 5 illustrates a scenario of CWR first price reverse auction. The CWR first price reverse auction is listed in Protocol 1.

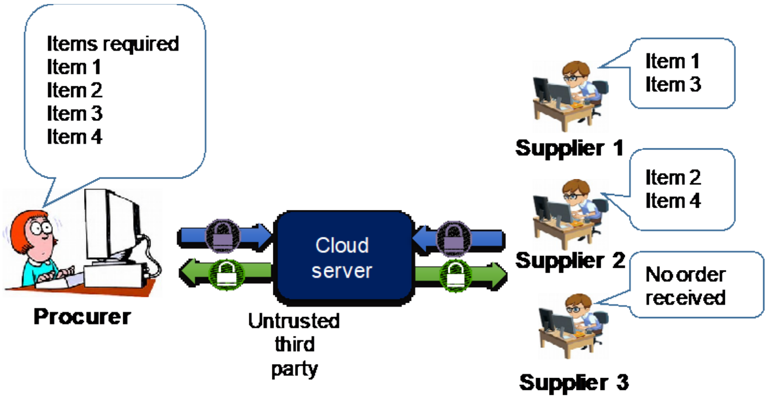


Figure 5. **CWR-First Price Reverse Auction**

The CWR first price reverse auction enables the procurer to learn only the payments that need to be made to each individual supplier and the items provided by each supplier. Throughout the protocol, the procurer cannot learn the supplier's individual item prices. Similarly, the supplier cannot learn the quantity desired by the procurer before the auction. The novelty in this protocol is that the external servers (cloud servers $\alpha, \beta,$ and γ) on which the CWR protocols are run do not know the auction's context (item names, etc.) as they receive morphed additive splits. Therefore, the external servers learn nothing about the procurer's/supplier's confidential information. Note that this protocol is designed to choose the supplier based on a single attribute of the product (price). This protocol can be extended to multiple attributes with the appropriate weights.

Implementation Details

Below are some of the details for implementing the CWR first price reverse auction:

1. **Secure Channels:** It is important to understand that information exchanges that occur between parties within the CWR auction should use secure channels, such as HTTPS.
2. **Cross Accounts:** The ownership of the cloud server account is one of the concerns while deploying CWR. Existing cloud servers, such as Amazon Web Services (AWS), offer features such as cross accounts through which a procurer and suppliers can examine what algorithms are being run on their data splits. Please refer the following webpage for more details: https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html
3. **Tie Breaks:** There is a possibility that the item prices of suppliers may be the same. In such scenarios, the procurer can break such ties in many ways, including randomly picking a supplier from the suppliers with the same item price. How such ties are handled is made public to all participants prior to the auction.
4. **Single Item Winner:** In some scenarios, a supplier may win only one item. This can reveal the item price to the procurer when he/she makes payments. In such scenarios, the corresponding supplier is informed and the supplier may choose to participate/quit the procurement process.

In the next section, we compare the performance of CWR-based computing techniques with competing secure computing techniques.

Performance Analysis of CWR

We developed a test-bench to run and compare different secure computing techniques such as partial homomorphic encryption and secret sharing, as discussed in the Overview of the Approach section. In what follows, we describe the test bed developed as part of this project to compare our approach (CWR) with the existing cryptographic approaches.

Test Bed Setup

We conducted experiments in two different settings. The first set of experiments was conducted when all the procurers and suppliers were connected to the same network (i.e., local area network or LAN). The second set of experiments was conducted when the procurers and suppliers were connected to different networks (i.e., wide area network or WAN). Note that the computation speed of all the approaches reduces with WAN. This is mainly attributed to the network latency.

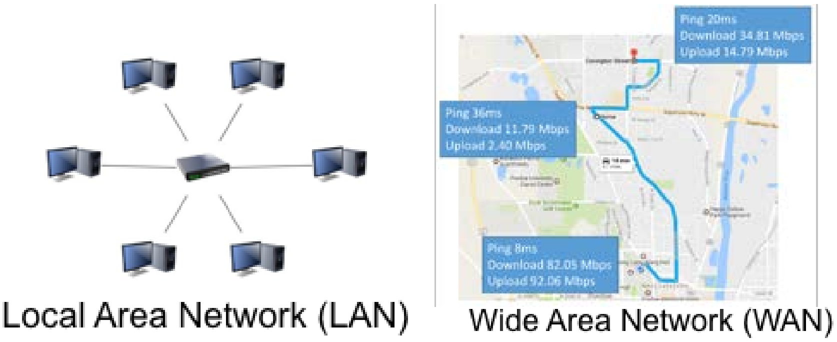


Figure 6. **Experimental Setup**

We identified computational time and bandwidth with respect to the amount of data that needs to be transferred between the procurer/suppliers as the key performance indicators (KPIs). The computational time is measured using a python module named “time” and the bandwidth is measured using an open source packet analyzer (Wireshark). We compared CWR protocols with competing secure computing techniques using these KPIs.

CWR-VIP

We chose the inner product as the computation to compare the performance of the proposed approach (CWR) against the existing approaches. This computation was chosen as it is commonly used to multiply the vector of quantity with the vector of item prices for the listed items within a procurement process.

We found that the proposed approach (CWR) is at least 10 times faster than the best existing approach (refer to Table 1) using LAN. We found that our approach is about 7 times faster than the best existing approach (see Table 2) using WAN. We realized that the cost of security (computational burden to maintain the confidentiality) in procurement activities is high (about 6–7 times) compared to open sharing, where procurement data is revealed to every participant. One of the reasons for this additional burden is the requirement of performing every computation using CWR protocols.

Table 1. Protocol Execution Time While Using LAN (in Seconds)

Vector length	0-server (PHE)	3-servers (Previous best) [9]	1-server (CWR-VIP)
10	14.6	4.1	0.35
100	135.5	37.4	2.88
1000	1738.4	378	27.5
10000	>3600	4031	264.7

Table 2. Protocol Execution Time While Using WAN (in Seconds)

Vector length	0-server (PHE)	3-servers (Previous best) [9]	1-server (CWR-VIP)
10	16.5	5.58	0.68
100	235	47.3	6.9
1000	>3600	486.3	74.7
10000	>3600	5567	742.6

In network communication, the amount of data (bandwidth) being exchanged between parties is another important performance indicator. In our comparative study, we found that our approach requires 3 times less bandwidth (refer to Table 3). These results indicate that our approach can be deployed in real-time applications and can be supported by devices with limited battery power.

Table 3. Comparison of Bandwidth Use (in KB)

Vector length	0-server (PHE)	3-servers (Previous best) [9]	1-server (CWR-VIP)
10	6.5	3.4	1.18
100	61.8	33.8	10.6
1000	614.2	342.7	105.9
10000	>5000	3425.3	1053.7

CWR-First Price Reverse Auction

We developed the software embodiment of the CWR-first price reverse auction (described in Protocol 1) and used it as an auction mechanism in a procurement process.

We used the values shown in Table 4 to simulate the auction mechanism. In what follows, we describe the outcomes of a traditional sealed bid auction and compare these outcomes with those obtained using CWR-first price reverse auction.

In a traditional sealed-bid auction, the procurer reveals the desired quantity. The suppliers submit their respective sealed bids ($330, $322, $316) to the procurer, who selects the minimum bid ($316) in first price auction and receives the items from Supplier 3. Throughout the auction process, suppliers hide their item prices in the form of sealed bids. However, from Table 4, we learn that Supplier 3 does not provide the best prices for each individual item.

Table 4. Item Prices and Quantities Used for Simulation Studies

Item Name	**Procurer** (Quantity)	**Supplier 1** (Item price)	**Supplier 2** (Item price)	**Supplier 3** (Item price)
A	12	$11	$9	$10
B	8	$6.5	$8	$7
C	7	$8	$6	$6.5
D	9	$10	$12	$10.5

Figure 7 shows a picture of the demo of this CWR-first price reverse auction, developed as part of this project. In this demo, one Microsoft SurfacePro computer was used as the procurer and three other SurfacePros were used as the suppliers to simulate a reverse auction. All the surface pros were connected with each other using 2 Mbps (upload/download speed) LAN. The procurer and suppliers mutually agree on three external servers ($\alpha, \beta, \text{and } \gamma$) which are used to run the CWR first price reverse auction. A computer is used to run these three external servers and this computer is also connected to all the SurfacePros using the same LAN.

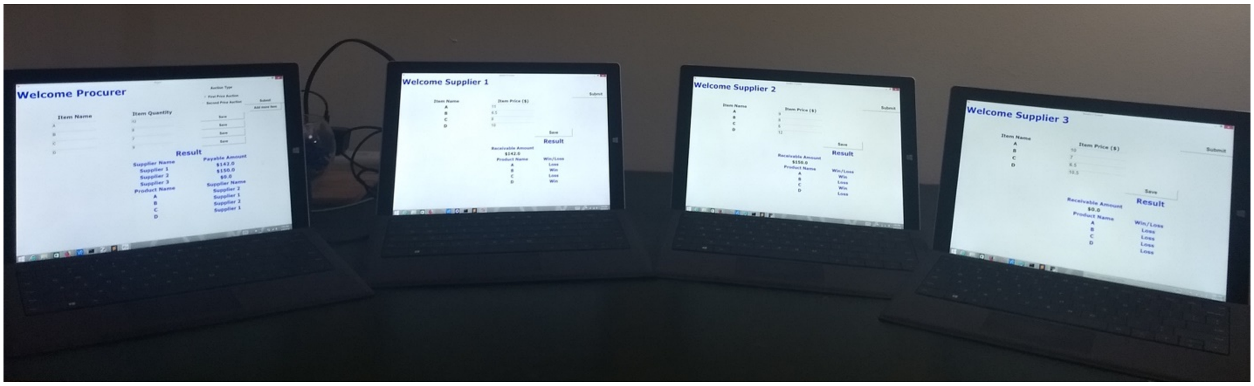
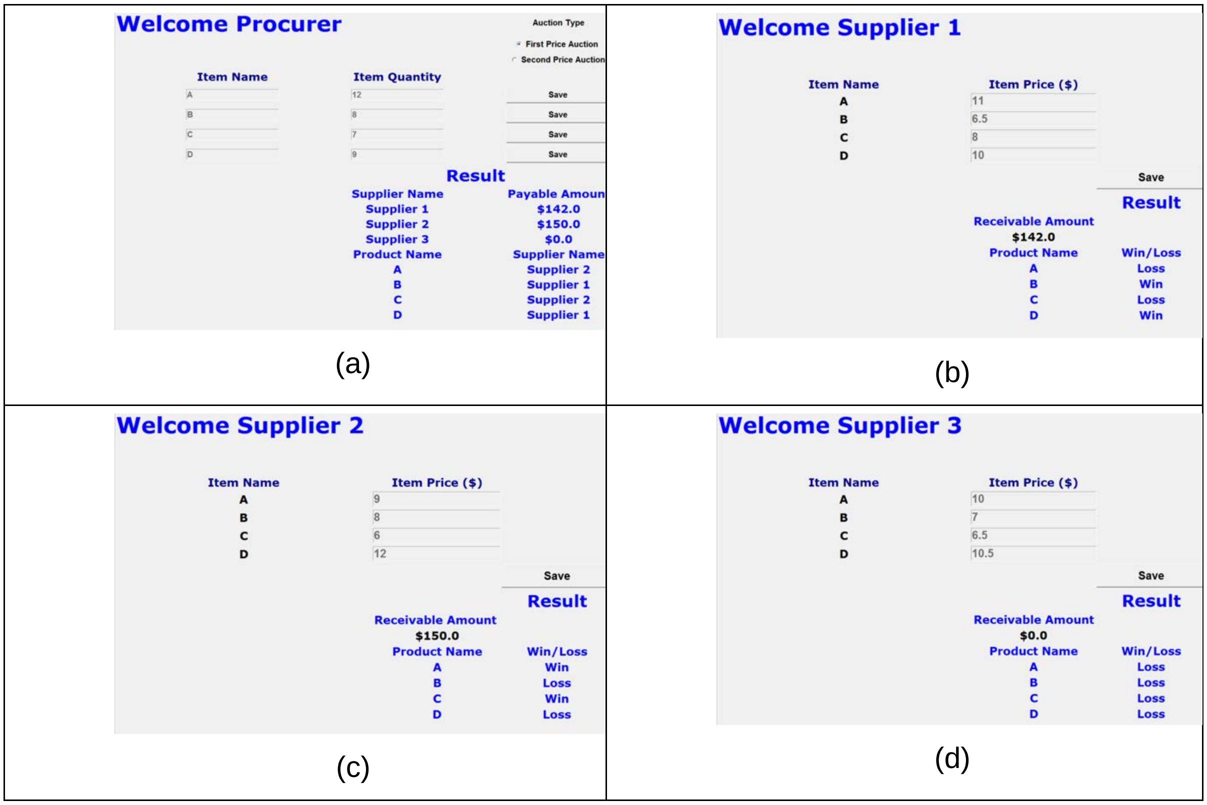


Figure 7. **Demo of a CWR-First Price Reverse Auction**

Deploying the CWR-first price reverse auction enables the procurer to enter item names and their respective quantities. Only the item names are provided to all the suppliers. Suppliers enter their respective confidential item prices (as listed in Table 4). As described in Protocol 1, the confidential information (item quantities and prices) is split additively and shared with the external servers ($\alpha \text{ and } \beta$). These external servers along with the help of another external server (γ) execute the computations involved in the auction. By the end of these computations, the procurer learns that items (A, C) and (B, D) will be provided by Supplier 2 and Supplier 1, respectively. The procurer also learns the amounts that should be paid to Supplier 1 and Supplier 2. The suppliers also receive information on the items they won/lost and their receivable payout amounts from the procurer. Figure 9 shows the screenshots of the procurer and suppliers at the end of the auction process. Note that throughout the procurement process, suppliers need not disclose their individual item prices to anyone.



(a)

Welcome Procurer

Auction Type

● First Price Auction

○ Second Price Auction

Item Name	Item Quantity	
A	12	Save
B	8	Save
C	7	Save
D	9	Save

Result

Supplier Name	Payable Amoun
Supplier 1	$142.0
Supplier 2	$150.0
Supplier 3	$0.0
Product Name	**Supplier Name**
A	Supplier 2
B	Supplier 1
C	Supplier 2
D	Supplier 1

(b)

Welcome Supplier 1

Item Name	Item Price ($)
A	11
B	6.5
C	8
D	10

Save

Result

Receivable Amount

$142.0

Product Name	Win/Loss
A	Loss
B	Win
C	Loss
D	Win

(c)

Welcome Supplier 2

Item Name	Item Price ($)
A	9
B	8
C	6
D	12

Save

Result

Receivable Amount

$150.0

Product Name	Win/Loss
A	Win
B	Loss
C	Win
D	Loss

(d)

Welcome Supplier 3

Item Name	Item Price ($)
A	10
B	7
C	6.5
D	10.5

Save

Result

Receivable Amount

$0.0

Product Name	Win/Loss
A	Loss
B	Loss
C	Loss
D	Loss

Figure 8. **Screenshots of the Procurer’s Screen (a) and the Suppliers’ Screens (b)–(d)**

This CWR-first price reverse auction enables procurers to select the suppliers who provide the best price for each individual item. Such selection enables the procurer to reduce procurement costs. For instance, using the values listed in Table 4, CWR-first price reverse auction enables the procurer to procure all the desired items for $292 instead of $316 (from traditional sealed-bid auctions). We believe that this form of cherry-picking enables the procurer to increase competition among suppliers and thereby achieve efficient solutions.

We extended the functionality of this software embodiment to handle second-price reverse auctions by modifying the calculation of payments in Protocol 1. We tested the scalability of the proposed CWR-first price reverse auction by running for different numbers of items procured by the procurer. The resulting computational time and bandwidth use are reported in Tables 5 and 6, respectively. These results indicate that CWR-first price reverse auction is a computationally efficient and secure technique that can be deployed in real-time settings.

Table 5. Comparison of Bandwidth Use (KB)

Number of items	CWR: First Price	CWR: Second Price
4	7.8	7.2
8	8.2	8.7
16	9.2	9.5
32	15.3	12.58
64	18.95	18.41

Table 6. Comparison of Average Computational Time (in Seconds)

Number of items	CWR: First Price	CWR: Second Price
4	0.05	0.06
8	0.11	0.13
16	0.21	0.22
32	0.40	0.42
64	0.76	0.82

The CWR-first price reverse auction is a step towards demonstrating that computations in a procurement process can be performed without needing to reveal any confidential information. We believe that procurers and suppliers can build on this and modify it to make it suitable for more sophisticated computations.

Summary

The proposed approach, Computing-Without-Revealing (CWR), supports research in information systems and risk management. Our approach also complements, but does not replace, research in economic mechanism design. While mechanism design is focused on truthful revelation through the design of incentives, our approach focuses on protecting confidential information in any mechanism. In this study, we developed new dedicated CWR protocols suited for eProcurement and demonstrated the application of these protocols for the procurement of standard products. We believe that these protocols could be extended to the procurement of innovative technologies.

We present the CWR-first price reverse auction, which enables a procurer to “cherry pick” those suppliers who provide the best price for each individual item and thereby lower procurement costs. Such lowering of acquisition costs for procurers will increase their efficiency because they will be able to achieve more with the same financial resources.

Suppliers who participate will not see their competitive advantage erode due to the very fact that they participated (e.g., currently, a cost advantage for some components quickly erodes once it becomes known). The eProcurement platforms based on the proposed approach will considerably mitigate the threat of data breach originating from business partners because the approach makes it possible to achieve the desired collaborative goals with business partners without revealing to them the confidential data on which the collaboration depends.

A test bed is developed to compare the performance of CWR-based protocols with the previous-best approaches. Experimental results show that the CWR protocols performed better than previous-best approaches. With this, we conclude that CWR based auctions are lightweight, scalable, and secure.

Protocol 1: CWR-First Price Reverse Auction

Input: Procurer provides the list of items (denoted by **I**) and their respective quantities (denoted by $\mathbf{q} = [q_1, \ldots, q_N]$). Suppliers ($S_1, \ldots, S_K$) provide their item prices for the items in the list **I**. Supplier S_k item price list is denoted by $\mathbf{p_k} = [p_{k1}, \ldots, p_{kN}]$.

Output: Procurer determines the items won (represented by $\mathbf{w_k}$) by each supplier S_k and payment (represented by a_k).

Stage 1. Pre-processing of inputs

Step 1: The procurer and suppliers mutually identify cloud servers (α and β) as their surrogates to execute procurement using CWR. The procurer splits their sensitive information $\mathbf{q}$ into $\mathbf{q}_\alpha$ and $\mathbf{q}_\beta$ such that $\mathbf{q} = \mathbf{q}_\alpha + \mathbf{q}_\beta$ and shares them with the cloud servers α and β, respectively; [[.]] notation is used to represent these shares, [[**q**]] represents $\mathbf{q}_\alpha$ for cloud server α and $\mathbf{q}_\beta$ for cloud server β respectively. Similarly, the suppliers split their individual item price list and share them with the cloud servers α and β, respectively.

Step 2: Cloud servers (α and β) mutually agree upon morphing functions (M_α, M_β) and a seed to generate the random numbers that are used in these morphing functions. These agreements can be derived using session number, auction ID, etc. Further, the cloud servers (α and β) identify another cloud server (γ) as their helper to perform the desired procurement computations using CWR.

Stage 2. Run desired computations securely

Step 3: Cloud servers ($\alpha, \beta,$ and γ) execute the computations as mentioned in Table 7. Cloud servers (α and β) keep track of the splits corresponding to the information on whether a supplier S_k won/lost the items ($\mathbf{w_{\alpha k}} = [w_{\alpha 1}, \ldots, w_{\alpha N}]$**,** $\mathbf{w_{\beta k}}$) and the splits corresponding to the payments that are to be made to the supplier S_k ($a_{\alpha k}$, $a_{\beta k}$). The vector ($\mathbf{w_k = w_{\alpha k}} + \mathbf{w_{\beta k}}$) has 1s against the items that are won and 0s against all the items lost by the supplier S_k.

Step 4: By the end of Step 3, cloud server α has ($\mathbf{a_\alpha} = [a_{\alpha 1}, \ldots, a_{\alpha k}]$, $\mathbf{W_\alpha} = [\mathbf{w_{\alpha 1}}, \ldots, \mathbf{w_{\alpha K}}]$) and cloud server β has ($\mathbf{a_\beta}$, $\mathbf{W_\beta}$)**.** Both cloud servers (α and β) share their splits with the procurer. The procurer adds ($\mathbf{a_\alpha}$**,** $\mathbf{a_\beta}$) to determine $\mathbf{a} = [a_1, \ldots, a_K]$ where a_k refers to the money that the procurer owes the supplier S_k. Similarly, the procurer adds **(**$\mathbf{W_\alpha}$, $\mathbf{W_\beta}$**)** to determine $\mathbf{W} = [\mathbf{w_1}, \ldots, \mathbf{w_K}]$.

Stage 3. Post-processing of outputs

Step 5: Procurers provide the payment a_K and items won (represented by $\mathbf{w_k}$) to S_k. Supplier S_k verifies the payment a_K against the item prices that he/she won.

Correctness

The correctness is derived from the correctness of CWR protocols.

Security

Procurer knows **q, a,** and **W**. With this information, the procurer cannot infer the suppliers' item prices. Similarly, suppliers receive $\mathbf{w_k}$ and the items they need to provide to the procurer. Additionally, the suppliers cannot infer each other's private information such as item price. All the external servers $(\alpha, \beta, \text{and } \gamma)$ receive only one of the additive splits. However, these external servers learn the number of suppliers participating in the auction. This could be avoided by using different external servers for the computations.

Table 7. Psuedocode for Computations Performed on Cloud servers (α and β)

```
N→ number of items
K→ number of sellers
[[P]]→ NxK matrix with additive shares corresponding to prices from sellers for different items
[[Q]]→ additive shares corresponding to the quantity from Buyer
Winner_price = [0] * N # winning price for each item
W = [[0] * N] * K # winner index
item_paycheck = [0] * N
for j in range(N):
    [[index]]=0 # make Seller 1 as the default winner
    for i in range(1, K):
        [[b]]=0 # [[b]] denotes an additive share of b
        W [j][index], lowest_price = 1, [[P[j][index]]]
        [[b]]←CWR-GT0(lowest_price – [[P[j][i]]]) # update indices and prices
        W[j][i], W[j][index] = [[b]], [[1-b]]
        [[index]]=CWR-ADD(CWR-MP([[b]], [[i]]), CWR-MP([[1-b]], [[index]]))
        [[Winner_price[j]]] = CWR-ADD(CWR-MP([[b]], [[P[j][i]]]), CWR-MP([[1-b]], [[lowest_price]]))
    [[item_paycheck[j]]] = CWR-MP([[q[j]]], [[Winner_price[j]]])
a=[0]*K
for j in range(K):
    for i in range(N):
        [[b1]] = 0
        [[b1]]←CWR-EW0(j, W[i][j])
        [[a[j]]] = CWR-ADD([[a[j]]], CWR-MP([[item_paycheck[i]]], [[b1]]))
```

References

Ben-David, A., Nisan, N., & Pinkas, B. (2008, October). FairplayMP: A system for secure multi-party computation. In *Proceedings of the 15th ACM Conference on Computer and Communications Security* (pp. 257–266). Alexandria, VA: ACM.

Bogdanov, D., Niitsoo, M., Toft, T., & Willemson, J. (2012). High-performance secure multi-party computation for data mining applications. *International Journal of Information Security*, *11*(6), 403–418.

Bogetoft, P., Christensen, D. L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., … Schwartzbach, M. (2009, February). Secure multiparty computation goes live. In *Proceedings of the International Conference on Financial Cryptography and Data Security* (pp. 325–343). Heidelberg, Germany: Springer.

Deshpande, V., Schwarz, L. B., Atallah, M. J., Blanton, M., & Frikken, K. B. (2010, October). Outsourcing manufacturing: Secure price-masking mechanisms for purchasing component parts. *Production and Operations Management, 20*(2), 165–180.

Kaestner, S., Arndt, C., & Dillon-Merrill, R. (2016, April). *The cybersecurity challenge in acquisition* (No. NPS-SYM-AM-16-041). Monterey, CA: Naval Postgraduate School.

Paillier, P. (1999, May). Public-key cryptosystems based on composite degree residuosity classes. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 223–238). Heidelberg, Germany: Springer.

Ponemon Institute. (2016, August). *Closing security gaps to protect corporate data: A study of US and European organizations.* Retrieved from https://info.varonis.com/hubfs/docs/research_reports/Varonis_Ponemon_2016_Report.pdf

Wang, S., Bhandari, S., Chaduvula, S. C., Atallah, M. J., Panchal, J. H., & Ramani, K. (2017, June). Secure collaboration in engineering systems design. *Journal of Computing and Information Science in Engineering, 17*(4), 041010–041010-11.

Wang, S., Nassar, M., Atallah, M., & Malluhi, Q. (2013, November). Secure and private outsourcing of shape-based feature extraction. In *International Conference on Information and Communications Security* (pp. 90–99). Cham, Switzerland: Springer.

Panel 8. Industrial Base Considerations Within Defense Acquisition

Wednesday, May 8, 2019	
2:15 p.m. – 3:30 p.m.	**Chair: David Stapleton,** Acting Deputy Assistant Secretary of Defense (Industrial Policy) ***Industrial Mobilization in World War I: Implications for Future Great Power Conflict*** Philip Koenig and Norbert Doerry, NAVSEA ***Microelectronics Industry Surety of Defense Supply: Policy Choices*** Gary Bliss, Institute for Defense Analyses ***Small Gas Turbine Engines: How Price and Quantity Affects Industrial Base Sustainment*** Patricia Bronson, Christopher Martin, and Brian Gladstone, Institute for Defense Analyses

David Stapleton—Mr. Stapleton currently serves as the Acting Deputy Assistant Secretary of Defense for Industrial Policy (IndPol). In this capacity, he is the principal advisor to the Under Secretary of Defense for Acquisition and Sustainment (A&S) for analyzing the capabilities, overall health, and policies concerning the industrial base on which the Department relies for current and future warfighting capabilities and requirements. IndPol is also responsible for developing the Department's position on the business combinations and transactions, both foreign and domestic, that shape and affect national security. Since becoming a member of the Department of Defense's Senior Executive Service in October 2016, he has undertaken an effort to protect and promote critical technology, infrastructure, and materials within the U.S. defense industrial base.

Mr. Stapleton started his career on Wall Street, where he last served as Vice President and Group Head of JPMorgan Investment and managed Market Strategy. He created a proprietary optimization methodology for advising Fortune 500 companies on asset class and fund allocations. During this time, he also guest lectured on the Economics of Finance at Columbia University. He most recently served in the private sector as the Chief Operating Officer of a startup technology company in Virginia.

Mr. Stapleton earned a B.A. from Georgetown, M.A. in International Relations from Columbia, J.D. from Northwestern and M.B.A. from the Wharton School, University of Pennsylvania.

Industrial Mobilization in World War I: Implications for Future Great Power Conflict

Norbert Doerry—is the Technical Director of the NAVSEA Technology Office (SEA 05T). In addition to leading special projects, Doerry facilitates the transition of technology from industry and academia into naval warships. He retired from active duty in the U.S. Navy as a Captain with 26 years of commissioned service. Dr. Doerry is currently focused on developing Medium Voltage DC (MVDC) Integrated Power and Energy Systems (IPES) for future warships, institutionalizing Set-Based Design in the U.S. Navy, and facilitating the introduction of flexibility and modularity features in future U.S. warships. [norbert.doerry@navy.mil and doerry@aol.com]

Philip Koenig—is the Director of the NAVSEA Industrial and Economic Analysis Division (SEA 05C1). His current work focuses on projections of cost, capability, and capacity in the U.S. shipbuilding industrial base. His previous experience was in the Future Ship and Force Architecture Concepts Division (SEA 05D1), the Office of Naval Research, NSWC Carderock, Chevron Shipping Company, and Vickers Shipbuilding Group Ltd. Dr. Koenig teaches shipbuilding courses at the University of British Columbia and at MIT. [philip.koenig@navy.mil and pckoenig@mit.edu]

Abstract

For approximately 25 years, the United States was the world’s sole superpower. With the emergence of China as a peer competitor on both the economic and military fronts, that era has come to an end. The prospect for near-future, industrial-scale, non-nuclear warfare can no longer be dismissed. Should that occur, it would be irresponsible to assume that a military decision would quickly ensue, therefore industrial (and societal) mobilization would be necessary. When considering this type of future, it is natural to look to the most recent historical example for guidance, and that would be World War II, in which America’s supremely effective industrial mobilization created the well-known “arsenal of democracy” that the enemy was not able to counter.

In this paper, we propose that while the World War II story is instructive, the run-up to World War I in which America’s industrial mobilization was far less effective, should not be ignored. This paper takes an introductory look at the failure of U.S. industrial mobilization in World War I, focusing on the case of shipbuilding. We review similarities and contrasts to today’s situation and suggest courses of action to reduce the likelihood of a similar outcome in the future.

Introduction

The total collapse of the Soviet Union in 1991, which took the West by surprise, thrust the United States into a new and unexpected role as the world’s sole superpower (Department of State, 2001–2009). The U.S. Navy suddenly exercised uncontested control of the high seas. Absent a high-end military threat, defense spending (including naval construction) was curtailed during the balance of the 1990s as resources were shifted to serve economic rather than military objectives. In that manner the American people looked forward to reaping a peace dividend. As the ex-Soviet fleet quickly deteriorated, the U.S. Navy’s principal role was re-directed toward projecting influence and power ashore. Following the attacks of September 11, 2001, the prospect of a peace dividend vanished as the military budget grew. But military operations in the post-911 era were focused on land warfare, and naval ship production rates did not expand appreciably. There was little urgency to developing plans to mobilize the shipbuilding industry in response to aggression from enemy naval forces capable of inflicting severe losses at sea.

This frame of mind ended in the mid- to late-2010s. The current geopolitical environment has become characterized by "overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations" (DoD, 2018). The result is a renewed potential for non-nuclear, industrial-scale war. If such a war were to break out against a peer-level enemy or against an alliance of multiple peer-level enemies, historical precedent suggests that demands on the U.S. Navy could quickly ratchet up.

The most recent major mobilization of the shipbuilding industry occurred prior to and during World War II. The World War II shipbuilding effort encompassed every type of naval and merchant ship, plus emergent types not envisioned prior to hostilities. The U.S. economy, directed and controlled by the State, performed brilliantly as described in an extensive literature that includes several recent book-length treatments (e.g., Wilson, 2016; Baime, 2015, & Herman, 2012) along with older classics such as Lane (1951), a standard text on the Emergency Shipbuilding Program of the Second World War.

The rapid and effective mobilization and expansion of war production (including shipbuilding) in World War II is a popular story due in part to its success, which was unprecedented. But the World War II effort was not original. It was preceded by a very similar push to mobilize U.S. industry, with a major focus on shipbuilding, in World War I. Responsible preparation for a future industrial-scale, non-nuclear war involving naval combat and trans-ocean supply lines would require an understanding of the World War I experience.

Shipping and Shipbuilding Actions Prior to U.S. Entry into the War

Prior to World War I, the world's dominant shipbuilder was Great Britain (see, for example, Stott, 2017).[1] At the early stages of the war, the British believed that the key maritime asset needed to defeat Germany was a large battle fleet, so naval construction was prioritized over merchant shipbuilding. Consequently, British commercial shipping deliveries actually dropped; the merchant ship tonnage delivered in 1915–1916 was only one third of that delivered in 1913–1914. French industry was unable to respond as resources were fully occupied in ground fighting. U.S. shipyards, which had been depressed prior to the war, responded and were quickly filled with new orders (Williams, 1989, pp. 38–41).

From 1915 to 1916, German U-boat action took a heavy toll as Germany attempted to counter-blockade Great Britain. In 1916 German submarines sunk one of four ships bound for the U.K. and continental Europe (Hutchins, 1948, p. 52). "By the spring of 1916, the amount of tonnage sunk each month by German U-Boats began to overtake the amount of new tonnage delivered" (Williams, 1989, p. 41). The most pressing need now was for cargo-carrying merchant ships. The British revised their industrial priorities; however, it was not enough. U.S. shipbuilding was needed to plug the gap.

The Shipping Act of 1916 established a new U.S. Shipping Board that was empowered and capitalized to form a subsidiary corporation for the purpose of building and

[1] Great Britain led the development of the steel shipbuilding industry, but its global market declined "from over 80% in the 1890s to zero by the end of the 1980s" (Stott, 2017).

operating merchant vessels. The Naval Act of 1916 provided for naval construction to be ramped up. Its general objective was to build a powerful battle fleet; motivated by battleship and battlecruiser action in the Battle of Jutland (May 31–June 1, 1916). Naval ships were constructed at the Navy yards and at the large, pre-existing private-sector shipyards, such as New York Shipbuilding (Camden, NJ), Newport News, Fore River, Union Iron Works, Bath Iron Works, William Cramp & Son, and Electric Boat.

The Three Sectors of the Shipbuilding Industry (New Construction)

The United States declared war on Germany on April 6, 1917, and this spurred industrial mobilization to build warships and merchant ships. The ship new construction industrial base comprised three sectors:

1. Navy yards
2. Existing commercial shipyards
3. Emergency commercial shipyards

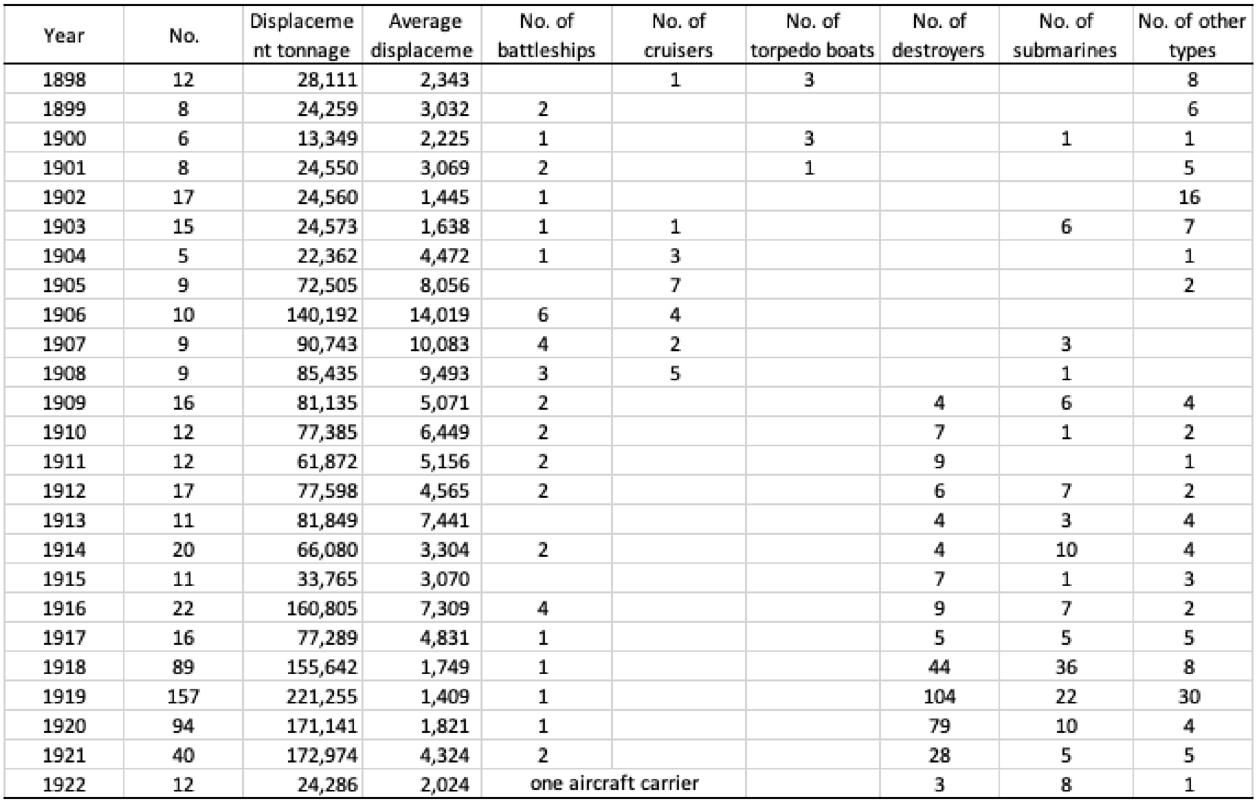
Each had distinct industrial characteristics and business bases. The Navy yards built warships, and the existing commercial shipyards built warships and a variety of merchant ship types. The emergency shipyards were a special case. Most, including the three largest, did not exist prior to the war. These emergency shipyards were “pop-up” facilities urgently constructed with government funding to build merchant ships quickly to overbalance the attrition from the German submarine campaign.

Naval Construction

Upon the entry of the United States into the war, naval shipbuilding underwent a complete change of plan in terms of both the quantity ordered and the mix of ship types. This is shown in Table 1, which traces U.S. naval ship production from shortly before the turn of the 20th century through World War I.

Table 1: Naval Vessels Delivered by Year, U.S., 1898–1922

(Smith & Brown, 1948, pp. 115–117)



Year	No.	Displacement tonnage	Average displaceme	No. of battleships	No. of cruisers	No. of torpedo boats	No. of destroyers	No. of submarines	No. of other types
1898	12	28,111	2,343		1	3			8
1899	8	24,259	3,032	2					6
1900	6	13,349	2,225	1		3		1	1
1901	8	24,550	3,069	2		1			5
1902	17	24,560	1,445	1					16
1903	15	24,573	1,638	1	1			6	7
1904	5	22,362	4,472	1	3				1
1905	9	72,505	8,056		7				2
1906	10	140,192	14,019	6	4				
1907	9	90,743	10,083	4	2			3	
1908	9	85,435	9,493	3	5			1	
1909	16	81,135	5,071	2			4	6	4
1910	12	77,385	6,449	2			7	1	2
1911	12	61,872	5,156	2			9		1
1912	17	77,598	4,565	2			6	7	2
1913	11	81,849	7,441				4	3	4
1914	20	66,080	3,304	2			4	10	4
1915	11	33,765	3,070				7	1	3
1916	22	160,805	7,309	4			9	7	2
1917	16	77,289	4,831	1			5	5	5
1918	89	155,642	1,749	1			44	36	8
1919	157	221,255	1,409	1			104	22	30
1920	94	171,141	1,821	1			79	10	4
1921	40	172,974	4,324	2			28	5	5
1922	12	24,286	2,024	one aircraft carrier			3	8	1

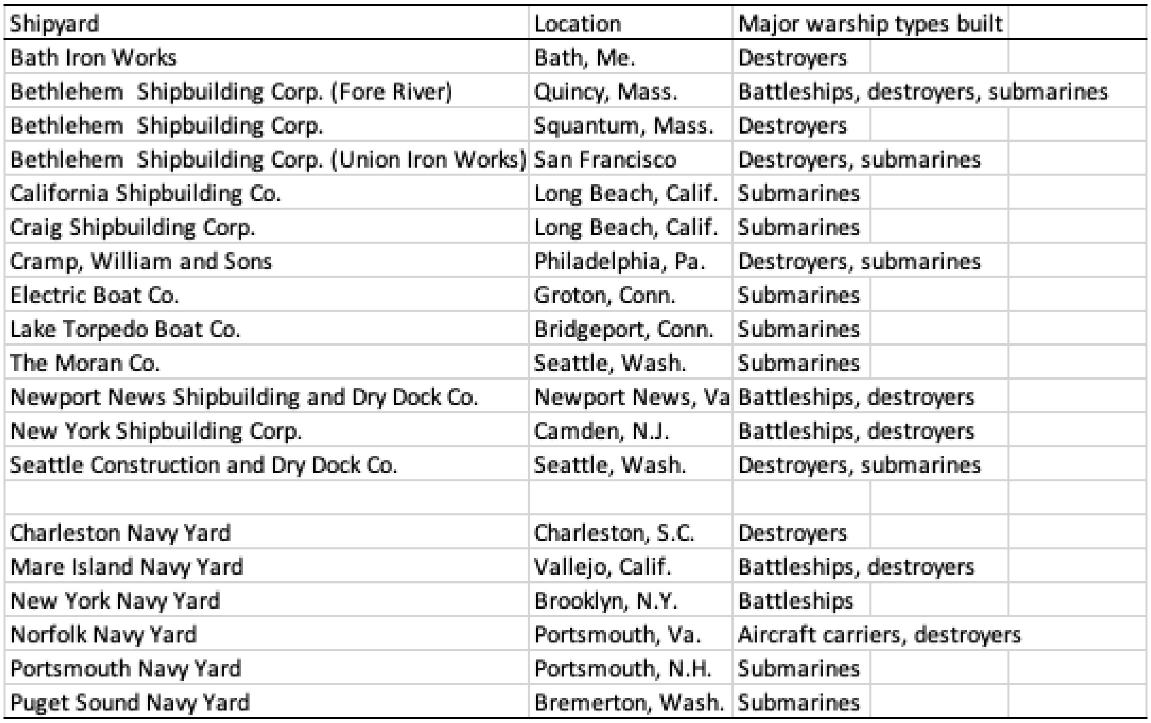
Note. Other types include minelayers, minesweepers, ammunition ships, fuel ships, tenders, monitors, and others.

Prior to World War I, the European great powers plus the United States and Japan had engaged in a naval arms race prominently geared towards fleet operations and featuring battleships and cruisers. Unexpectedly for all belligerents, World War I naval combat followed a different course. Table 1 shows that the U.S. Navy shipbuilding plan was revamped to prioritize destroyers and submarines rather than capital ships, but the re-orientation and the ramp-up did not happen quickly enough. While the armistice was signed in 1918, peak output was not reached until 1919.

The major naval fighting ships (battleships, destroyers, and submarines) were built at a variety of shipyards including all three types, that is, Navy yards, existing private sector yards, and a new emergency yard, as shown in Table 2. The emergency shipyard that was purpose-built for destroyer production was the Navy-owned, Bethlehem Shipbuilding Corporation-operated facility at Squantum, MA. That yard followed the concept of the merchant ship emergency yards and was designed to build a single ship-type (destroyers) in large numbers. The shipbuilding supplier industries required rapid expansion along with the shipyards. For example, in conjunction with the construction of the new Squantum shipyard, the Navy also built a new boiler shop in Providence, RI, and a turbine shop in Buffalo, NY. The Navy financed facilities expansion at other existing shipyards, including the Newport News shipyard and the New York Shipbuilding Corporation yard in Camden, NJ, along with expansions to other critical suppliers such as Erie Forge (DoN, 1921).

Table 2: Shipyards That Built Major Warship Types From 1913 to 1922

(Smith & Brown, 1948, p. 132)



Shipyard	Location	Major warship types built
Bath Iron Works	Bath, Me.	Destroyers
Bethlehem Shipbuilding Corp. (Fore River)	Quincy, Mass.	Battleships, destroyers, submarines
Bethlehem Shipbuilding Corp.	Squantum, Mass.	Destroyers
Bethlehem Shipbuilding Corp. (Union Iron Works)	San Francisco	Destroyers, submarines
California Shipbuilding Co.	Long Beach, Calif.	Submarines
Craig Shipbuilding Corp.	Long Beach, Calif.	Submarines
Cramp, William and Sons	Philadelphia, Pa.	Destroyers, submarines
Electric Boat Co.	Groton, Conn.	Submarines
Lake Torpedo Boat Co.	Bridgeport, Conn.	Submarines
The Moran Co.	Seattle, Wash.	Submarines
Newport News Shipbuilding and Dry Dock Co.	Newport News, Va	Battleships, destroyers
New York Shipbuilding Corp.	Camden, N.J.	Battleships, destroyers
Seattle Construction and Dry Dock Co.	Seattle, Wash.	Destroyers, submarines
Charleston Navy Yard	Charleston, S.C.	Destroyers
Mare Island Navy Yard	Vallejo, Calif.	Battleships, destroyers
New York Navy Yard	Brooklyn, N.Y.	Battleships
Norfolk Navy Yard	Portsmouth, Va.	Aircraft carriers, destroyers
Portsmouth Navy Yard	Portsmouth, N.H.	Submarines
Puget Sound Navy Yard	Bremerton, Wash.	Submarines

Note. Shown are shipyards that built battleships, destroyers, and submarines, i.e., the principal fighting ships. No cruisers were built in this period.

Merchant Ship Construction

The U.S. shipbuilding industry had become very active following the 1914 outbreak of the war, as the British shipyards were filled to capacity with orders. On April 16, 1917, 10 days after the declaration of war on Germany, the U.S. Shipping Board created the Emergency Fleet Corporation; all of the shares were held by the Shipping Board. The Shipping Board was essentially regulative, with the Emergency Fleet Corporation being its operational arm. The initial organization of the Shipping Board was badly flawed, leading to unresolvable technical and managerial disputes at the top level. In late July 1917, senior leadership was replaced with a more effective line-up and the World War I shipbuilding program got under way in earnest. But the political and bureaucratic paralysis cost the program four months that proved impossible to recover.

On July 11, 1917, under its new and more energetic leadership, the Emergency Fleet Corporation took control of the U.S. shipping and shipbuilding industries. It requisitioned all 431 steel merchant ships under construction in U.S. shipyards, totaling 3,068,431 deadweight tons (Hutchins, 1948). This was not enough however, and what followed was “the greatest flood of ship orders in American history. The task was indeed the largest shipbuilding effort in the world’s history up to that time” (Hutchins, 1948, p. 52). It is worth quoting Hutchins at length here:

> In 1917, before the entry of the United States into the war, the shipbuilding industry had already grown to forty-two yards with 154 ways for steel ships. … Before 1914, about 75 per cent of the country’s shipyard capacity was normally engaged in naval work. By 1919, however, the capacity had risen to seventy-two steel shipyards with 461 ways. … The

yards were then engaged in the construction of more commercial than naval tonnage.[2] (Smith & Brown, 1948)

The need far exceeded the capacity of the existing shipbuilding industry.[3] The construction of new emergency shipyards and the enlargement of existing ones was necessary. Hurley (1927) described the situation as follows:[4]

> Originally it was supposed that the main function of the Fleet Corporation would be that of developing designs and placing contracts for ships. But all the yards were either busy in completing for the Fleet Corporation the 431 hulls which we had commandeered, or were clogged with orders for the Navy. The shipyard owners, found that they could not control the supply of either material or labor. Hence the Fleet Corporation had to step in and manage the yards. Entirely new yards had to be built, at an expense so huge that it could not be defrayed by private companies. In the end the Fleet Corporation had to build the yards with government money and to act as their banker.

The Emergency Fleet Corporation contracted for three new large shipyards to be built by private-sector firms. The largest was the Hog Island shipyard in Philadelphia.[5] This facility was owned by the American International Corporation, which also owned the huge, modern New York Shipbuilding Corporation yard in Camden, NJ. Hog Island (and the other purpose-built yards) built ships to a standard design, employing newly conceived prefabrication methods on a massive scale. Hog Island “built 122 ships of 921,000 deadweight tons between the laying of the first keel … on Feb. 12, 1918 and the completion of its last vessel on Jan. 29, 1921, averaging a keel every 5.5 days.” Of those 122 ships, 110 were of the pre-fabricated standard Hog Island 7,600 dwt freighter. The yard had 50 slipways but not as many shop facilities as a conventional shipyard, as many parts and components were manufactured elsewhere. Peak employment was 30,000. (Hutchins, 1948, pp. 54–55; Goldberg, 1991, pp. 3–14). See Table 3 for a summary of activity at the Emergency Fleet Corporation shipyards.

[2] Table 10 lists the 70-odd shipyards.

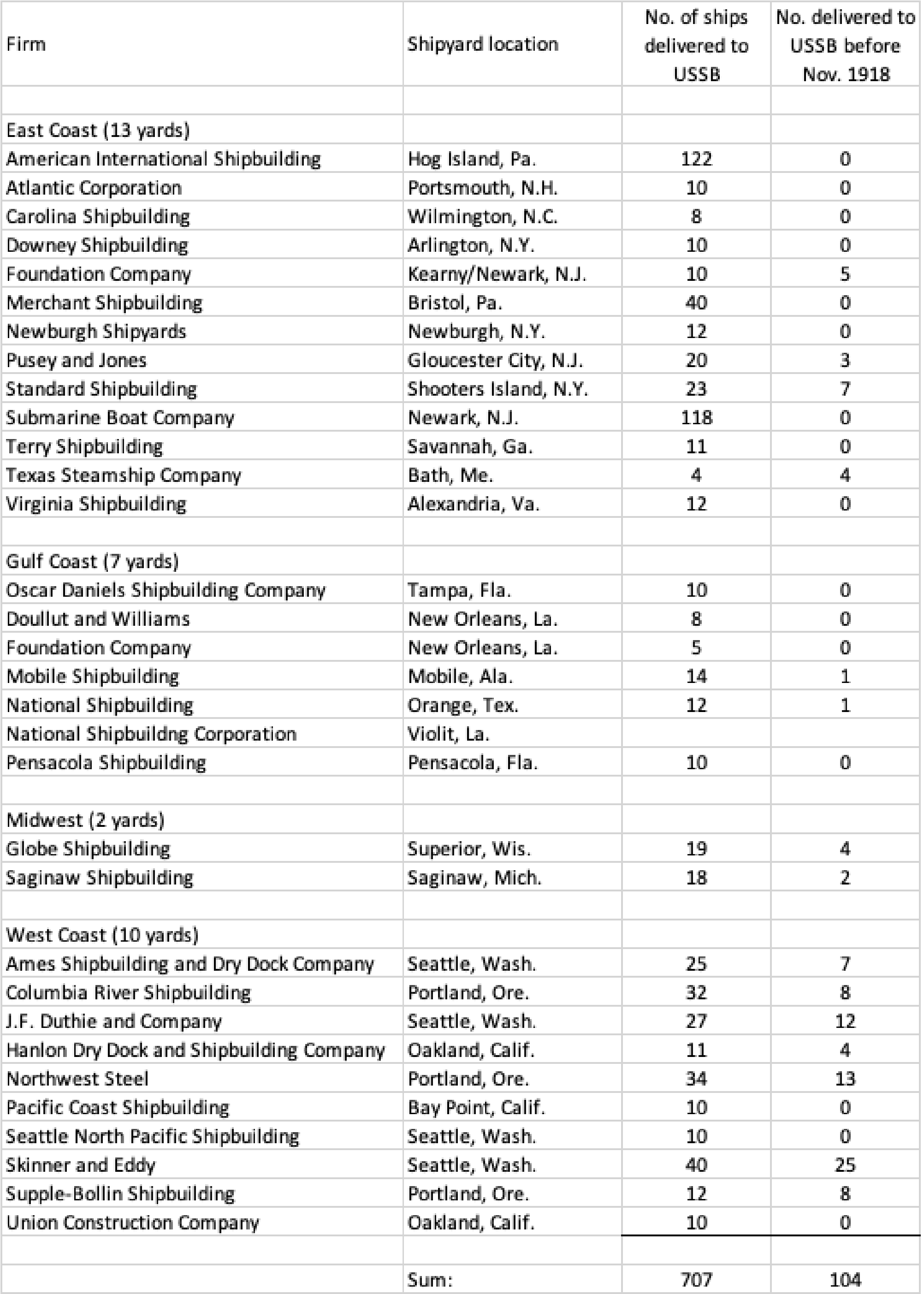
[3] Merchant ships were so desperately needed that the Shipping Board placed orders in Japanese and Chinese shipyards (Goldberg, 1991, p. 3).

[4] Edward N. Hurley was appointed chairman of the U.S. Shipping Board in July 1917 as part of the USSB’s reorganization.

[5] The others were the Newark shipyard of the Submarine Boat Company and the Bristol, PA, yard of the Merchant Shipbuilding Corporation.

Table 3: World War I Emergency Shipyards

(Shipbuildinghistory.com, Tim Colton, accessed Feb. 13, 2019)



Firm	Shipyard location	No. of ships delivered to USSB	No. delivered to USSB before Nov. 1918
East Coast (13 yards)			
American International Shipbuilding	Hog Island, Pa.	122	0
Atlantic Corporation	Portsmouth, N.H.	10	0
Carolina Shipbuilding	Wilmington, N.C.	8	0
Downey Shipbuilding	Arlington, N.Y.	10	0
Foundation Company	Kearny/Newark, N.J.	10	5
Merchant Shipbuilding	Bristol, Pa.	40	0
Newburgh Shipyards	Newburgh, N.Y.	12	0
Pusey and Jones	Gloucester City, N.J.	20	3
Standard Shipbuilding	Shooters Island, N.Y.	23	7
Submarine Boat Company	Newark, N.J.	118	0
Terry Shipbuilding	Savannah, Ga.	11	0
Texas Steamship Company	Bath, Me.	4	4
Virginia Shipbuilding	Alexandria, Va.	12	0
Gulf Coast (7 yards)			
Oscar Daniels Shipbuilding Company	Tampa, Fla.	10	0
Doullut and Williams	New Orleans, La.	8	0
Foundation Company	New Orleans, La.	5	0
Mobile Shipbuilding	Mobile, Ala.	14	1
National Shipbuilding	Orange, Tex.	12	1
National Shipbuildng Corporation	Violit, La.		
Pensacola Shipbuilding	Pensacola, Fla.	10	0
Midwest (2 yards)			
Globe Shipbuilding	Superior, Wis.	19	4
Saginaw Shipbuilding	Saginaw, Mich.	18	2
West Coast (10 yards)			
Ames Shipbuilding and Dry Dock Company	Seattle, Wash.	25	7
Columbia River Shipbuilding	Portland, Ore.	32	8
J.F. Duthie and Company	Seattle, Wash.	27	12
Hanlon Dry Dock and Shipbuilding Company	Oakland, Calif.	11	4
Northwest Steel	Portland, Ore.	34	13
Pacific Coast Shipbuilding	Bay Point, Calif.	10	0
Seattle North Pacific Shipbuilding	Seattle, Wash.	10	0
Skinner and Eddy	Seattle, Wash.	40	25
Supple-Bollin Shipbuilding	Portland, Ore.	12	8
Union Construction Company	Oakland, Calif.	10	0
	Sum:	707	104

Note.

1. A few of these yards completed a small number of later ships, for example, USSB cancellations that they were able to complete for private-sector ship owners.
2. Dozens of cargo ships were delivered to the French government by various emergency shipyards.
3. A few additional emergency yards built smaller ships of less than 1,000 gross tons.

As seen in Table 3, the Hog Island shipyard achieved a prodigious output. But its first ship, the *Quistconck*, was delivered in December 1918, too late for World War I service.[6] This must have been a colossal frustration at the time, and it is the general theme of the World War I merchant and naval shipbuilding effort: technically impressive, far in front of shipbuilding thinking elsewhere in the world, but ultimately did not contribute to victory in the war. The Hog Island shipyard was promptly closed down and demolished after the last delivery in 1921; much of the site is now the Philadelphia airport. However, the effort was a valuable dress rehearsal for World War II, in which the same theme of ship manufacturing in huge, purpose-built facilities was adopted with much more timeliness.

The merchant shipbuilding program's results in Table 3 paralleled those of the naval construction program: impressive industrial mobilization, but too late for most of the ships to come on line during the war (see Figure 1). This effect was exacerbated in the merchant vessel program, as most of the shipyards did not exist before the hostilities, and the largest did not exist until after U.S. entry.

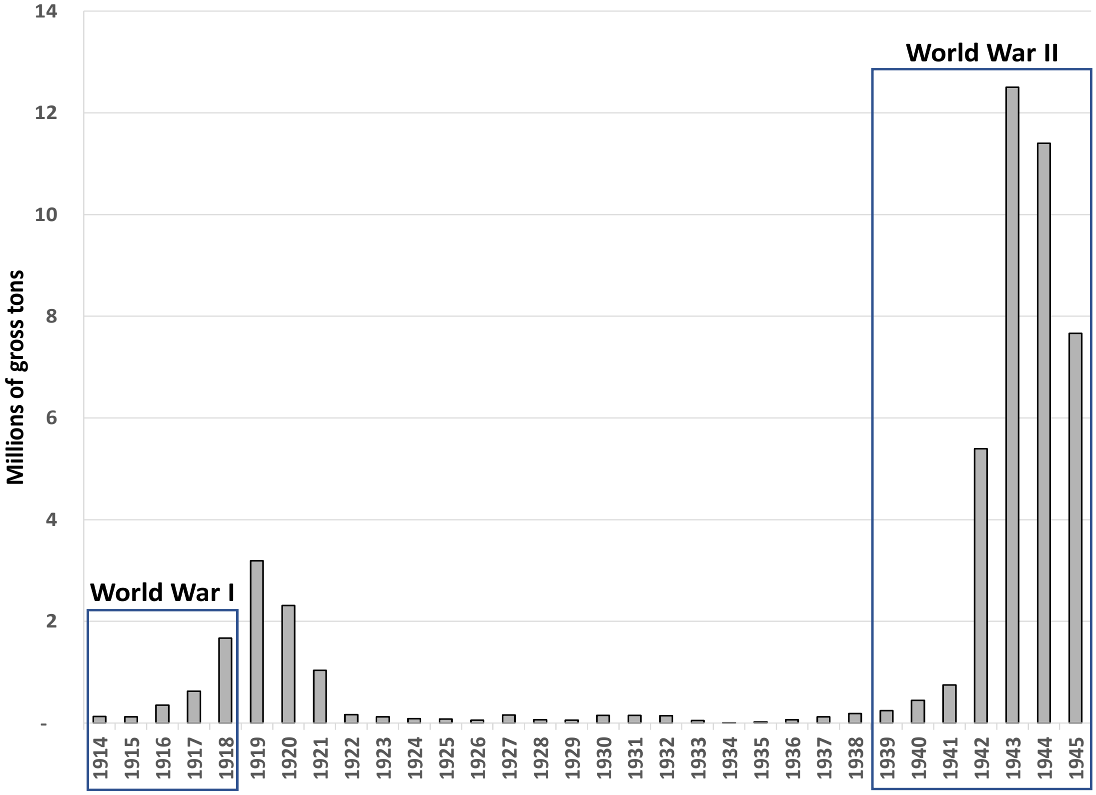


Figure 1. **Gross Tons of Steel Merchant Ships (over 2,000 gt) Delivered 1914–1945**
(Smith & Brown, 1948)

[6] See http://www.shipbuildinghistory.com/shipyards/emergencylarge/aisc.htm. Accessed Feb. 11, 2019.

Discussion and Recommendations

The U.S. World War I shipbuilding program was not effective because it started well after World War I was underway, and because of poor management in its initial stages. World War I began in August 1914, and by the end of that year it was clear that it would be a long desperate struggle, yet the United States made few preparations for naval construction until the Naval Act of 1916. Seven months later, in April 1917, the United States entered the war, and at that point the Emergency Fleet Corporation still had not been created.

The contrast to the World War II experience is stark. A ramp-up in ship orders for that war started at the expiration of the naval arms limitation treaties in 1936, three years prior to European theatre hostilities. As early as 1939, efforts were initiated to expand industrial capacity. During America's pre-War period (1936–1941), 182 destroyers were authorized and 39 were delivered.

The World War I experience suggests some food for thought in preparation for the onset of future industrial-scale, non-nuclear, global war. A few samples are offered in the next paragraphs.

1. Investments in options could increase industrial capacity rapidly. This would include the shipbuilding industrial base and the critical supplier base of facilities that take the same general timeframe to ramp up as a shipyard. This could include foundries, forges, specialty machine shops, and other types of production facilities, and capacity for development of software infrastructure for naval and commercial ships.
2. Merchant marine and merchant shipbuilding policies may be due for a reexamination. In past global wars, merchant fleets have been instrumental tools of military strategy. They were required to reposition ground forces, their gear, and supplies between overseas theatres of war. The U.S. merchant marine has substantially atrophied since World War II. U.S. subsidy programs supporting the foreign trading segment of the merchant marine have not been funded since the early 1980s.[7] Before 1914, approximately 75% of U.S. shipbuilding industrial capacity was engaged in Navy new construction. But at the height of World War I, after tremendous capacity expansion, there were more merchant ships being built than warships even though most of the warships being built were small. In World Wars I and II, at the point when the situation was grimmest for the allied powers, merchant shipbuilding was by far the #1 priority, not warship construction.
3. In preparation for high-volume wartime production, creation of detailed designs of merchant and naval ship types could be done in advance. If the two world wars are valid guidance (not known), then other ship types, including long-lead-time warships, would out of necessity be placed at lower priority.[8] The corollary would be that those are the ship types that would be emphasized in peacetime in the absence of war exigencies.

[7] The foreign trading segment of the merchant marine exists outside of the Jones Act legislative environment. Historically it was supported via mechanisms including subsidies and cargo preference programs (Gibson & Donovan, 2000).

[8] World War I lasted less than 4 ½ years (including prior to U.S. involvement), so even for the European belligerents, no ships that took longer than that to build were able to be used during the war.

4. Prototype construction of some of those ship designs to work out design issues, production issues, and gain feedback from the operator for design mods may be an effective way to smooth the path to wartime volume production. For effective designs, it may be advantageous to store jigs and other critical tooling.
5. Ship design flexibility may be at a premium at the outset of a new industrial-scale conflict, due to the impossibility of accurately predicting the nature of future naval combat. In World War I, not only was the naval surface combatant production priority changed from capital ships to destroyers, the originally intended fleet combat role of the destroyers (e.g., torpedo attacks on enemy capital ships) never materialized. Instead, they were pressed into service convoying merchant vessels and conducting the world's first antisubmarine warfare campaign (Gardiner, 1985).

Conclusion

The industrial mobilization experience of the United States in World War II has been described and discussed in an extensive literature and is well known. One reason is that it is an uplifting story, and in significant ways it embodied the ideals upon which the best in American civilization is based. It was as the "arsenal of democracy" that America made, arguably, its most irreplaceable contribution to allied victory. A critical lynchpin of that effort was shipbuilding, where the result was achieved through the voluntary, dedicated labor of an unprecedented cross section of American society (including women and minorities) who were effectively mobilized with a common goal of building merchant ships to counter the effects of German submarine warfare.

In World War I, both the need and the means were almost the same, and yet the result was disappointing, even though the United States responded in a spectacular fashion, temporarily becoming the largest shipbuilding nation in the world, and the ships built during the World War I program "composed the great bulk of the American merchant marine until the construction program of World War II had effect" (Hutchins, 1948, p. 53). In this paper we have described the actions taken and that the results were too late to have as much effect as they could have had.

For an additional cautionary conclusion, we now take a big-picture look. We observe that the industrial mobilization outcome in the 1941–1945 war was fully informed by the 1917–1918 experience. For World War II, "the characteristics of that earlier period were … again duplicated" (Hutchins, 1948, p. 57). In terms of industrial base strategy, industrial organization, and manufacturing technology, World War I served almost as a dress rehearsal for World War II. In a potential 21st century non-nuclear World War III, could the United States update the successful World War II script to achieve victory? Not likely, as too many variables (industrial, economic, geopolitical) have undergone fundamental change since 1945. Which brings us back to the World War I predicament: mobilizing the industrial base in a new economic environment, for a new type of war.

References

Baime, A. J. (2015). *The arsenal of democracy: FDR, Detroit, and an epic quest to arm an America at war.* Boston, MA: Mariner Books.

DoD. (2018). *Summary of the 2018 National Defense Strategy of the United States of America.* Retrieved from https://www.defense.gov/Portals/1/Documents/pubs/2 018-National-Defense-Strategy-Summary.pdf

DoN. (1921). *Activities of the bureau of yards and docks: World War, 1917–1918*. Washington, DC: Government Printing Office.

Department of State. (2001–2009). Dissolution of the USSR and the establishment of independent republics, 1991 (U.S. Department of State Archive, January 20, 2001–January 20, 2009). Retrieved from https://2001-2009.state.gov/r/pa/ho/time/pcw/108229.htm

Fasset, F. G., Jr. (1948). *The shipbuilding business in the United States of America, Vol. I.* New York, NY: Society of Naval Architects and Marine Engineers.

Gardiner, R., & Gray, R. (1985). *Conway's all the world's fighting ships 1906–1921*. Annapolis, MD: Naval Institute Press.

Gibson, A., & Donovan, A. (2000). *The abandoned ocean: A history of United States maritime policy*. Columbia, SC: University of South Carolina Press.

Goldberg, M. H. (1991). *The "Hog Islanders": The story of 122 American ships*. Kings Point, NY: American Merchant Marine Museum.

Herman, A. (2012). *Freedom's forge: How American business produced victory in World War II*. New York, NY: Random House.

Hurley, E. N. (1927). *The bridge to France.* Philadelphia, PA: J. B. Lippincott.

Hutchins, J. G. B. (1948). History and development of the shipbuilding industry in the United States. In F. G. Fasset, Jr. (Ed.), *The shipbuilding business in the United States of America, Vol. I* (Ch. II)*.* New York, NY: Society of Naval Architects and Marine Engineers.

Lane, F. C. (1951). *Ships for victory: A history of shipbuilding under the U.S. Maritime Commission in World War II*. Baltimore, MD: Johns Hopkins University Press.

Smith, H. G., & Brown, L. C. (1948). Shipyard statistics. In F. G. Fasset, Jr. (Ed.), *The shipbuilding business in the United States of America, Vol. I* (Ch. III)*.* New York, NY: Society of Naval Architects and Marine Engineers.

Stott, P. (2017, November 8). Shipbuilding in Britain: How to reboot it. *The Conversation*. Retrieved from http://theconversation.com/shipbuilding-in-britain-how-to-reboot-it-87031

Williams, W. J. (1989). *Shipbuilding and the Wilson Administration: The Development of Policy, 1914–1917* (Doctoral dissertation). Ann Arbor, MI: University of Washington*.*

Wilson, M. R. (2016). *Destructive creation: American business and the winning of World War II*. Philadelphia, PA: University of Pennsylvania Press.

Acknowledgments

We wish to acknowledge the encouragement and support of Jill Boward, Director, NAVSEA Cost Engineering and Industrial Analysis Group, and of Tim Barnard, Director, NAVSEA Technology Group.

Panel 9. Autonomous Systems Acquisition—Challenges for the DoD

Wednesday, May 8, 2019	
2:15 p.m. – 3:30 p.m	**Chair: Paul Mann,** Technical Director, Naval Surface Warfare Center, Port Hueneme Division ***A Framework for Aligning Emerging Small UAS Technologies With Defense Acquisition Processes*** Jonathan Wong, RAND Corporation ***Technology Trust: The Impact of Trust Metrics on the Adoption of Autonomous Systems Used in High Risk Applications*** Michael Anderson, SPAWAR, and Johnathan Mun, Naval Postgraduate School ***When Does It Make Sense to Acquire a Single Weapon System Design That Can Be Used in Both Manned and Unmanned Operational Modes?*** Prashant Patel and David Tate, Institute for Defense Analyses

Paul Mann—Mr. Mann was appointed to Senior Executive Service (SES) in 2010 and is currently Division Technical Director for Naval Surface Warfare Center, Port Hueneme Division (NSWC PHD). In this role, he oversees execution of the division's technical capabilities, program planning, technical authority, workforce development, and strategic investments.

Prior to his role at NSWC PHD, Mr. Mann served as Acting Principal Deputy Director for the DoD Test Resource Management Center and led execution of statutory and regulatory responsibilities, including a Major Range and Test Facility Base capability assessment, strategic planning, congressional reports, Test and Evaluation (T&E) infrastructure investments and DoD T&E budget certification. He also completed a fouryear assignment at White Sands Missile Range as the Executive Technical Director leading all Joint T&E responsibilities.

During his first SES role, he supported the Under Secretary of Defense for Acquisition, Technology, and Logistics as the Assistant Deputy Director for Land Warfare Portfolio of Major Programs. Prior, he executed a 50-month tour as Joint Program Manager, leading procurement, fielding, and sustainment for the Mine Resistant Ambush Protected (MRAP) Vehicles Program at Marine Corps Systems Command, Quantico, Va. With budget growth during his tour from $900 million to more than $44 billion, MRAP became the highest priority acquisition program in the DoD, successfully delivering more than 27,000 vehicles to two theaters of operation.

Mr. Mann previously had successful tours at Naval Sea Systems Command as Division Director (SEA 61) for Warfare Systems Engineering and Architecture, and Division Director (SEA 62) for Force Readiness, Test, and Certification under the Warfare Systems Engineering Directorate (SEA 06). He led expansion of the Navy Distributed Engineering Plant, and collaborated with weapon and ship program offices and fleet stakeholders to deliver readiness. As the Aegis Deputy Technical Director (PMS 400B1), Mr. Mann delivered air defense capability and managed missile integration in Aegis ships, including projects in Foreign Military Sales.

His decorations include the Army Meritorious Civilian Service Award, the Secretary of Defense Medal for Meritorious Civilian Service, a Joint Meritorious Unit Citation, the Rear Adm. Wayne E. Meyer Memorial Award for Acquisition Excellence, the David Packard Excellence in Acquisition Award for JPO MRAP, two Navy Superior Civilian Service Awards and multiple performance and excellence awards.

Mr. Mann earned his Bachelor of Science in mathematics, cum laude, from the University of La Verne and also holds a Master of Public Administration from the Key Executive Leadership Program at American University in Washington, D.C.

A Framework for Aligning Emerging Small UAS Technologies With Defense Acquisition Processes

Jonathan Wong—PhD**,** is an Associate Policy Researcher at the RAND Corporation. Wong's research focuses on military force development issues such as the role of new technologies, processes, and concepts in shaping how militaries fight. He is a former management consultant and Marine Corps infantryman. [jonwong@rand.org]

Joslyn Fleming—is a Policy Analyst at the RAND corporation, where she focuses on logistics, military readiness, and personnel policy. She is a former Marine Corps supply officer and a current reserve civil affairs officer. [jfleming@rand.org]

Abstract

Small unmanned aircraft systems (SUAS) are increasingly important for ground combat operations. SUAS extend ground unit situational awareness and their ability to prosecute targets, and may enhance command and control. Their fast development cycles, commercial availability, and still-maturing operational concepts, though, do not align well with conventional U.S. Department of Defense (DoD) force development processes and timelines. This paper proposes a framework to address this misalignment by rapidly capturing unstructured qualitative insights on SUAS usage and converting them into procurement and allocation levels within the context of existing force development processes. The process leverages semi-structured interviews and document collection for data collection, followed by a mixed method approach using qualitative coding and mathematical matching. The result is a set of procurement and allocation levels that balances current operational needs with opportunities for experimentation and concept development.

Introduction

Current Marine Corps operations and future operating concepts place a heavy emphasis on disaggregated and distributed operations (U.S. Marine Corps, 2016). Such operations require high demand, low density capabilities such as aerial imagery and command, control, communications, computers (C4) assets to provide battlefield awareness. Currently, the Marine Corps centralizes many of these assets at regimental or higher echelons. This approach is inadequate to provide support to subordinate units conducting disaggregated and distributed operations. As such, the Marine Corps has seen an increased demand for organic means of enhancing battlespace awareness at the company level and below. To meet this growing demand, the Marine Corps has invested in emerging small unmanned aircraft system (SUAS) technology which provides small units with not only organic situational awareness capabilities, but also other capabilities that were once exclusively held at higher level units. The Marine Corps has been experimenting with these platforms for over 15 years and has accelerated its efforts to integrate SUAS into operations.

However, the Marine Corps is still refining its requirements for this maturing technology. The analyses that drive requirements are incomplete. Other platforms have been acquired through the rapid acquisition process. The current acquisition approach has focused on ground combat elements, primarily infantry units, but the expectation is that other unit requirements will expand rapidly when other elements are considered.

Additionally, SUAS technology advances are being influenced by commercial factors that may crowd out military ones.[1]

The Marine Corps has identified that a comprehensive review of the SUAS portfolio is required. This review will help determine what capabilities are needed across the Marine Air Ground Task Force (MAGTF) and where there are current gaps. The purpose of this research is to document lessons learned from the Marine Corps' recent experience and recommend next steps in SUAS allocation and procurement.

Research Approach

For this research, SUAS are defined as unmanned aircraft systems (UASs) in Department of Defense (DoD) UAS Groups 1 and 2; these systems weigh less than 55 pounds, fly lower than 3,500 feet above ground level (AGL), and fly no faster than 250 knots. Groups 1 and 2 encompass a wide span of capabilities. We further define SUAS using the seven emerging categories used by U.S. Special Operations Command (USSOCOM) Expeditionary Organic Tactical AISR Capability Set (EOTACS) to further refine DoD Groups 1 and 2.[2] These seven categories are explained in Table 1. In particular, we use the performance characteristics of each EOTACS category to frame our procurement analyses and recommendations in later chapters. Note that Category 1 consists of tethered platforms and is not considered SUAS and thus not considered in our research.

[1] Facilitator interview

[2] AISR: airborne intelligence, surveillance, reconnaissance

Table 1. USSOCOM EOTACS Categories Considered in This Analysis
(U.S. Special Operations Command, 2018)

		Categories					
Characteristic	**Threshold Specification**	**2 Nano VTOL**	**3 Micro VTOL**	**4 SR/SE VTOL**	**5 SR/SE FW**	**6 MR/ME FW**	**7 LR/LE FW**
Payload	Electro-optical/infrared (EO/IR)?	Yes	Yes	Yes	Yes	Yes	Yes
	Payload threshold weight (lbs)	0	0	1	1	2	10
Endurance	Endurance (hours)	0.2	0.2	0.5	0.5	2	6
Speed	Cruise (knots-indicated air speed, KIAS)	10	15	20	20	25	25
	Dash (KIAS)	10	15	20	35	35	35
Weight	Min (lbs)	0	0	3	0	0	20
	Max (lbs)	1	3	10	20	20	55
Launch	Hand?	Yes	Yes	Yes	Yes	Yes	Yes
	Rail?	No	No	No	Yes	Yes	Yes
	Vertical Take-off and Landing (VTOL?)	No	No	No	Yes	Yes	Yes
	Bungee	No	No	No	No	No	Yes
	Tether?	No	No	No	No	No	No
Recovery	Runway-independent?	Yes	Yes	Yes	Yes	Yes	Yes
	Deep stall?	No	No	No	Yes	Yes	Yes
	Sliding (belly land)?	No	No	No	Yes	Yes	Yes
	Combination?	No	No	No	Yes	Yes	Yes

Note. VTOL: vertical takeoff and landing, FW: fixed wing, SR: short range, SE: short endurance, MR: medium range, ME: medium endurance, LR: long range, LE: long endurance

Assumptions and Limitations

Like any research, this effort was bounded by various assumptions and practical constraints. We identify them here at the outset of this report.

- This research only addresses SUAS needs for CE and GCE units from the squad to regimental level.
- This research is confined to examining material solutions.
- The mathematical matching methodology errs on the side of inclusivity when it comes to linking SUAS platforms and categories to definable mission tasks.
- This analysis is budget-unconstrained as it assesses CE and GCE SUAS employment today, along with future needs, and develops an idealized future state to inform decision makers considering future SUAS procurement.
- Costs are representative of current models for each category and are current as of October 2018.
- Procurement recommendations do not include platforms already in Marine Corps possession.

- We did not consider the effect that task-organized units (i.e., Marine air ground task forces) might have on reducing the number of platforms needed.
- At the request of the sponsor, our quantities do not take attrition or additional maintenance float requirements into consideration.

A Literature Review Identified Decision Paths and Outcomes of Actions That the Marine Corps Has Already Taken

To capture the Marine Corps' baseline SUAS usage, we reviewed a variety of after action reviews (AARs), reports, and open-source literature to understand the work that the Marine Corps has already done to develop its SUAS capability. This body of work spanned over 10 years and helped us understand the previous analyses, decisions, and problem areas that have informed the Marine Corps' SUAS efforts. In particular, they helped us identify five mission profiles that encompass the different ways the Marine Corps may use SUAS (exemplar sources are cited):

- **Situational awareness:** Increase small-unit commanders' ability to visualize the battlefield to speed their decision-making process (Dalby, 2013).
- **Force protection:** At the small-unit level, provide standoff detection ability to detect and inspect improvised explosive devices (IEDs) or unexploded ordnance (UXO) to allow freedom of maneuver (Gillis, 2017).
- **Rapid target engagement:** Increase small-unit commanders' ability to identify, locate, and engage targets, particularly time-sensitive ones (Dalby, 2013).
- **Persistent C4:** Increase small units' abilities to communicate through voice and data, particularly at beyond line of sight (LOS) ranges or dense terrain that suppresses signals (NCOs, SNCOs, & Officers of 3d Bn 5th Marines, 2017).
- **Persistent electronic warfare (EW):** Provide small units with the ability to sense and affect the electromagnetic spectrum for military purposes (Turnbull, 2019).

Semi-Structured Interviews and Qualitative Coding Systematically Revealed Operational Insights From Current Users

To assess how well the Marine Corps is employing its SUAS to fulfill those mission profiles today, we conducted and analyzed a series of semi-structured interviews. Interviews provided direct access to personnel intimately involved in managing and employing SUAS. We developed and followed semi-structured protocols that encouraged discussion about how SUAS are currently employed, how they might be employed in the future, the force development process, and sustainment. We opted for semi-structured interviews to encourage greater consistency across interviewees while allowing the flexibility to explore relevant subject areas that we did not anticipate during protocol development. Our literature review suggested three different interview groups, and our protocols were tailored to focus on areas most relevant to each:[3]

- **Sponsors** that articulated how the SUAS serves Marine Corps purposes. This included HQMC(CD&I) and PMA-263. Protocols focused on future employment, force development, and sustainment.

[3] Although we focused on certain interview areas for each group, all groups were given the opportunity to discuss all interview areas.

- **Facilitators** that enable SUAS employment, such as training and logistics support agencies (TALSAs), MCTOG, VMXs, and Defense Innovation Unit (DIU). Protocols were focused on force development and sustainment.
- **Operators** that employ the SUAS, which mostly consisted of unit SUAS program managers from division to battalion level.[4] Protocols were focused on current employment, future employment, and sustainment.

We interviewed 69 individuals across 39 organizations between May and November 2018. We conducted interviews in person at Marine Corps and DoD installations across the continental United States (CONUS) and over the phone. In addition to interviewing HQMC sponsor and facilitator organizations, we interviewed at least one unit of each type from the CE and GCE.

Thematic Analysis

We explored the collected literature review and interview data through qualitative coding and thematic analysis. To ground our analysis. we developed a code tree with themes we were interested in exploring. The code tree was based on initial themes that emerged from the literature and interviews, including the utility of various SUAS mission profiles, preferred SUAS design characteristics, employment, and sustainment issues. All interviews were coded by two team members using Dedoose thematic analysis software (De Vries et al., 2008).[5] This activity was particularly important in enabling us to quantify the qualitative data captured in the interviews (e.g., priority of SUAS design characteristics) and understand its ordinality. In addition, coding captured tones and sentiments that helped us more comprehensively understand the underlying connotations interviewees associated with various aspects of SUAS. Emergent relationships observed in coding were used to guide and inform other aspects of the research approach.

The interview results, in conjunction with the review of source documentation, allowed us to examine a variety of themes across and between different interviewee perspectives (e.g., HQMC versus operating forces, CE versus GCE, and different OccFlds and echelons). This analysis forms our assessment of the current state of SUAS in the Marine Corps, explored in the following three themes.

Mathematical Matching Helped Identify the Best SUAS for Each OccFld and Echelon

To systematically relate the insights from the literature review and interview themes into procurement and allocation recommendations, we took several steps to convert the qualitative data into quantitative proxies. We used a mathematical matching method to transform the qualitive data into ideal SUAS design characteristics for each occupational field (OccFld) and echelon, then allocated them to CE and GCE units. This yielded a set of procurement and allocation courses of action for the Marine Corps to consider. Model inputs can be changed, allowing the Marine Corps to conduct additional analysis using different assumptions or units of interest.

[4] Although we interfaced with units no smaller than battalions, they provided us with access or perspective on lower echelons, down to the squad level.

[5] To ensure consistency of coding by all coders, inter-rater reliability was tested using Cohen’s kappa. The two coders involved in this project achieved a 0.91 kappa score, indicating almost perfect agreement.

Complementary Data Sources Shaped the Ideal SUAS Profile for Each OccFld and Echelon

To convert the qualitative data into quantitative proxies, we considered three additional data sets to give depth and rigor to the process:

- The 1,242 training and readiness (T&R) tasks that define tasks for each OccFld and echelon of interest
- EOTACS framework, including representative costs
- Descriptions of the five SUAS mission profiles

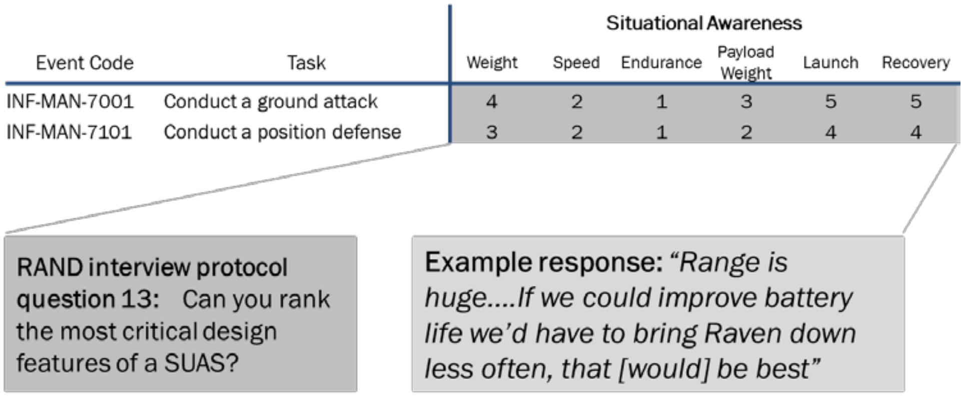
Each data source complements the others, forming a broad understanding of how SUAS may be useful for a given OccFld-echelon combination. T&R tasks define the entire range of tasks that a given OccFld-echelon combination is required to perform, but do not offer information about how SUAS might fit into a task. Interview data provided information on how SUAS might help an OccFld-echelon combination perform its mission generally, but not at the detailed level described in the T&R manual. The EOTACS framework helps us delineate different levels of capability between SUAS. Lastly, the SUAS mission profiles paint a detailed picture of how SUAS might help with Marine Corps missions generally but does not characterize how they might help any given OccFld-echelon combination.

Combining the data allowed us to articulate the ideal SUAS design profile for each OccFld-echelon combination. Note that interview inputs were necessarily limited to ordinal preferences and some design characteristics were subjective.[6] To accommodate this (and to make the ideal SUAS design profile relatable to existing classes of SUAS), we converted all preference data into rankings of the importance of each design characteristic for each T&R task for each mission profile.[7]

For instance, consider the infantry battalion task of conducting a ground attack (T&R task INF-MAN-7001). Rankings were informed by interview inputs and the research team’s understanding of each T&R task definition and mission profile description. On that basis, SUAS situational awareness capabilities would be useful in this regard, but not force protection, rapid target engagement, persistent C4, or persistent EW. Within the situational awareness task, a SUAS’ endurance is the most important priority. Speed is the next priority, followed by payload carrying capacity, weight, and launch and recovery flexibility. This process was repeated for all 1,242 T&R tasks related to the OccFlds and echelons of interest for this research. If a task did not apply to a mission profile, then it was assigned a null value. See Figure 1 for a graphical example.

[6] For instance, it would be difficult for an interviewee to articulate a response to our question about design preferences with a numeric answer such as specific speed or payload carrying capacity. Rather, we asked for a general ranking of the design characteristic. Nevertheless, an ordinal preference does not indicate how close either ideal specifications or platforms might be to each other. In reality, platforms might be quite comparable, but ordinal rankings force a distinct prioritization, which could distort choices.

[7] Embedded in each individual T&R task is the OccFld and echelon that it applies to; no T&R task is applied to more than one OccFld echelon combination.



Event Code	Task	Situational Awareness Weight	Speed	Endurance	Payload Weight	Launch	Recovery
INF-MAN-7001	Conduct a ground attack	4	2	1	3	5	5
INF-MAN-7101	Conduct a position defense	3	2	1	2	4	4

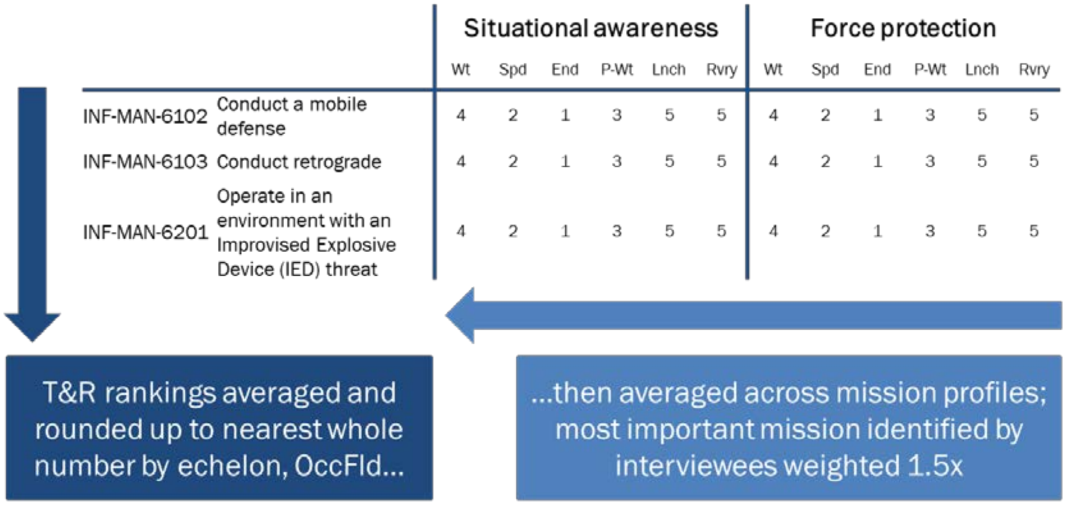
RAND interview protocol question 13: Can you rank the most critical design features of a SUAS?

Example response: *"Range is huge....If we could improve battery life we'd have to bring Raven down less often, that [would] be best"*

Figure 1. **Example of Training & Readiness SUAS Design Characteristic Ranking**

Note. Source: RAND analysis

The result was a set of 37,260 individual ranking sets.[8] To generalize this information down to an ideal SUAS profile, we took the average of all ranking sets for each OccFld-echelon combination. Note that we considered all T&R tasks to be equally important to the overall functioning of an OccFld-echelon combination.[9] However, we did consider the relative importance of each mission profile to each OccFld-echelon combination. In this case, we opted to weight the situational awareness mission 1.5 times the other mission profiles, as it was the one that was most consistently mentioned in interviews. The ultimate result is a ranking of the importance of the six SUAS design characteristics for each OccFld-echelon combination. See Figure 2 for a graphical example.



		Situational awareness						Force protection					
		Wt	Spd	End	P-Wt	Lnch	Rvry	Wt	Spd	End	P-Wt	Lnch	Rvry
INF-MAN-6102	Conduct a mobile defense	4	2	1	3	5	5	4	2	1	3	5	5
INF-MAN-6103	Conduct retrograde	4	2	1	3	5	5	4	2	1	3	5	5
INF-MAN-6201	Operate in an environment with an Improvised Explosive Device (IED) threat	4	2	1	3	5	5	4	2	1	3	5	5

T&R rankings averaged and rounded up to nearest whole number by echelon, OccFld...

...then averaged across mission profiles; most important mission identified by interviewees weighted 1.5x

Figure 2. **Aggregating Preference Inputs Into Ideal SUAS Profiles**

[8] From 1,242 rankings multiplied by six design characteristics, multiplied by five mission profiles.

[9] This can be reinvestigated by other, more knowledgeable experts if needed.

Note. Source: RAND analysis

Matching Ideal Profile to SUAS Design Characteristics

The next step is to identify the EOTACS category that best meets the ideal design profile articulated by a given OccFld-echelon combination. To do this, we used a common method for ranking complex preferences, known as the analytical hierarchy process (AHP), with some modifications.

We Modified an Analytical Hierarchy Process to Accommodate Ranked Preferences

The standard AHP takes as its inputs matrices of pairwise comparisons between characteristics (Satty, 1986). These pairwise comparisons specify which of each pair is more suitable—and by how much—according to a prescribed mapping of verbal descriptions of relative suitability to numeric scores.

In standard AHP, the verbal descriptions enable analysts to directly compare the direction and magnitude between a pairwise comparison.[10] Since our interviewees were only able to respond with design preferences in ranked order, we modified the AHP methodology by expressing a unit's numerical capability requirement profile as a single vector ranking the relative importance of each SUAS characteristic. Similarly, because units have not had the opportunity to establish specific platform-agnostic technical specifications, we converted the technical specifications of platform categories to rankings of each category for each characteristic. For example, the category with the fastest speed was ranked 1 for speed. See Table 2 for a graphical depiction of this arrangement.

Table 2. Ranked SUAS Design Characteristics

Design characteristic	**Directionality**	**Cat 1 Tethered**	**Cat 2 Nano VTOL**	**Cat 3 Micro VTOL**	**Cat 4 SR/SE VTOL**	**Cat 5 SR/SE FW**	**Cat 6 MR/ME FW**	**Cat 7 LR/LE FW**
Endurance	Longer is better	1	5	5	4	4	3	2
Speed	Faster is better	5	4	3	2	2	1	1
Weight	Less is better	6	1	2	3	4	4	5
Payload capacity	Heavier is better	2	4	4	3	3	2	1
Launch	More options are better	3	2	2	2	1	1	1
Recovery	More options are better	3	2	2	2	1	1	1

Note. Source: RAND analysis

We next applied the modified AHP algorithm to compare the ideal SUAS profiles to the converted EOTACS categories. Our modified algorithm was originally developed in R

[10] For example, consider an interview with a car enthusiast about engine preferences. The interviewee can respond with specific horsepower or liter displacement preferences. Since these design preferences can be articulated as quantitative values, the direction and magnitude of the preferences (expressed as Euclidian distances) can be evaluated directly.

and later adapted to VBA to facilitate wider compatibility with USMC computers. The following steps illustrate each transformation in the algorithm:

- Ranked EOTACS profile is read in and reversed such that higher values represent better performance in a category. This was done to facilitate modified pairwise comparisons.
- Aggregated unit preference averages are read in using the VBA macro.
- A pairwise matrix is constructed by taking the ratio of each ranked design characteristic to each other. For example, the weighted rank for endurance is compared to the weighted rank for payload carrying capacity by dividing the weighted rank score by the weighted endurance score. The matrix yields 36 ratios, which are then summed by column.
- A normalized matrix is created by dividing each cell value from the modified pairwise matrix by the sum of the respective column from the same matrix. The average of each row yields the weight of a given design characteristic for each OccFld-echelon combination.
- The dot-product of the design characteristic categories for each SUAS and the weight vector created in the previous step yields a score value for each EOTACS category. The highest score indicates the optimal match.

The process is repeated for each OccFld-echelon combination. The resulting scores yield a complete ranking of each EOTACS category to each OccFld-echelon combination from best to worst fit.

These analytical outputs are not prescriptive. Like any process, we expect the modified AHP to have some shortcomings (see the next section), given how much we reduced and generalized the starting inputs. Rather, these outputs should be considered as the starting point for further evaluation of the optimal EOTACS category for a given OccFld-echelon combination.

Modified AHP Has Some Shortcomings

Our modified AHP reduces match quality by compressing both the Euclidean distance between units with different priorities and between SUAS categories with different capabilities.[11] In this specific application, these modifications likely did not affect match results because SUAS categories vary most significantly along discrete dimensions, such as whether a category offers vertical take-off and landing (VTOL). As the SUAS market matures and more specialized platforms become available, users can increase the fidelity of this model by

[11] For example, consider comparisons between two different pairs of platforms along the dimension of endurance. Suppose that for the first pair, the highest ranked platform has a maximum endurance of 10 hours and the second ranked platform has an endurance of 9.5 hours. Suppose that for the second pair, the top ranked is 10 hours and the second ranked is only five hours. The endurance of the first pair is so close that it might be preferable to go with the second ranked platform if, for example, it is significantly less expensive or superior along another performance dimension such as speed. In contrast, the difference between the second pair is significant, and the first platform is likely preferable for a unit requiring longer endurance, even at the expense of greater cost or other performance features. Our modified AHP cannot distinguish between these two situations in the same way the standard AHP with pairwise rankings can.

- establishing capability-based, platform-agnostic technical requirements where possible (i.e., the maximum acceptable decibel signature for a unit) for subsequent use in a quantitative matching algorithm, and
- where requirements cannot be expressed in quantitative terms, generating full pair-wise comparison matrices in order to employ the standard AHP, rather than ranking across characteristics.

To identify the SUAS categories best satisfying unit capability requirements, we input both the SUAS category capability rankings and unit capability requirements profiles into the AHP algorithm, which mathematically identified the best matched SUAS category for each unit's capability requirements profile.

We Developed Quantity Recommendations From Literature Review and Interview Inputs

Having identified the best EOTACS category (or categories) for each OccFld and echelon, we estimated the total quantity of platforms needed to usefully carry out the missions that SUAS might be useful for. For each OccFld-echelon combination, we considered interview inputs, unit AARs, unit CONEMP and CONOP slides, the Marine Operating Concept, and current unit organization documents to identify the needed quantity of each EOTACS category. In some cases, some OccFlds had highly developed CONEMPs and CONOPs that illustrate concepts and plans for how SUAS might be employed within the context of an operation. These slides often included recommended quantities and types of SUAS needed to accomplish a given mission. In other cases, we had to infer and estimate the number.[12] We then scaled that quantity up so as to equip all units in a given OccFld-echelon combination. Finally, we considered a slightly reduced allocation to capitalize on the Marine Corps' existing TALSA investments to manage a pooled SUAS fleet for units that are less mature in their SUAS employment concepts.

Results

Our results are divided into two sections. First, qualitative insights on the current state of SUAS in the Marine Corps indicate a greater need for access to platforms in order to fully determine what the optimum quantity and type of SUAS might be. Second, we offer a set of three procurement and allocation recommendations that fulfill the access need to varying degrees.

Current State of SUAS in the Marine Corps

The thematic analysis identified three key results about the current state of SUAS in the Marine Corps.

Marine Corps Occupational Fields Only Partially Grasp What SUAS Mission Profiles Are Useful to Them

Based on our thematic analysis, we found that Marine Corps CE and GCE units understand and value the utility of some SUAS mission profiles, but the utility of other

[12] We inferred quantities in such cases by reviewing doctrine, T&R standards, and emerging concepts (described in the Marine Operating Concept) to identify how many of each type of SUAS would need to be used by a given unit and how many units would have to employ SUAS simultaneously.

profiles remains unclear. Recall from the Research Approach chapter that the Marine Corps identified five mission profiles: (1) situational awareness, (2) force protection, (3) rapid target engagement, (4) persistent C4, and (5) persistent EW. Almost all units shared numerous and substantial observations about situational awareness and force protection mission profiles. When asked how their units currently employ SUAS, interviewees discussed tasks that corresponded to the situational awareness mission profile 97 times in 29 of 42 interviews. Tasks related to the force protection mission profile were mentioned 51 times in 32 interviews. One excerpt from a light armored reconnaissance (LAR) unit indicates the familiarity and appreciation for the ability of SUAS to enhance situational awareness:

> I think the situational awareness … the idea behind [the RQ-11B Raven] is for preliminary reconnaissance before the vehicles go up. See the route, identify manmade or natural obstacles and whether or not we should even try.

Even units that did not have much experience with SUAS shared substantive observations about how they *would* employ SUAS for these mission profiles. A reconnaissance interviewee who had only used SUAS sporadically in the past illustrates a level of appreciation for it, much the same as we saw in the previous excerpt:

> [The] key benefit is providing offset from our objective[;] it avoids big compromise problems. It allows us to gather information without being close.

Another interviewee from an artillery unit (a community that did not indicate frequent SUAS usage) discussed both its usage for situational awareness as it is described in this context and also for understanding its own force signature:

> [We use SUAS] to fly red cell. Training batteries use them to understand new threat dimension, to look to the sky. This is not something were used to thinking about. We do lots of red cell work, [as well as] assessment of our own signature, what we look like.

These and other responses indicate that CE and GCE units understand how SUAS can enable both mission profiles and what the concepts of employment may entail.

However, the other three mission profiles were less frequently commented on or understood. Rapid target engagement was mentioned 56 times, but only in 13 interviews. Interestingly, some units professed deep experience in using SUAS for rapid target engagement, but others did not. An infantry interview excerpt illustrates the almost casual and pedestrian nature of using SUAS for this mission:

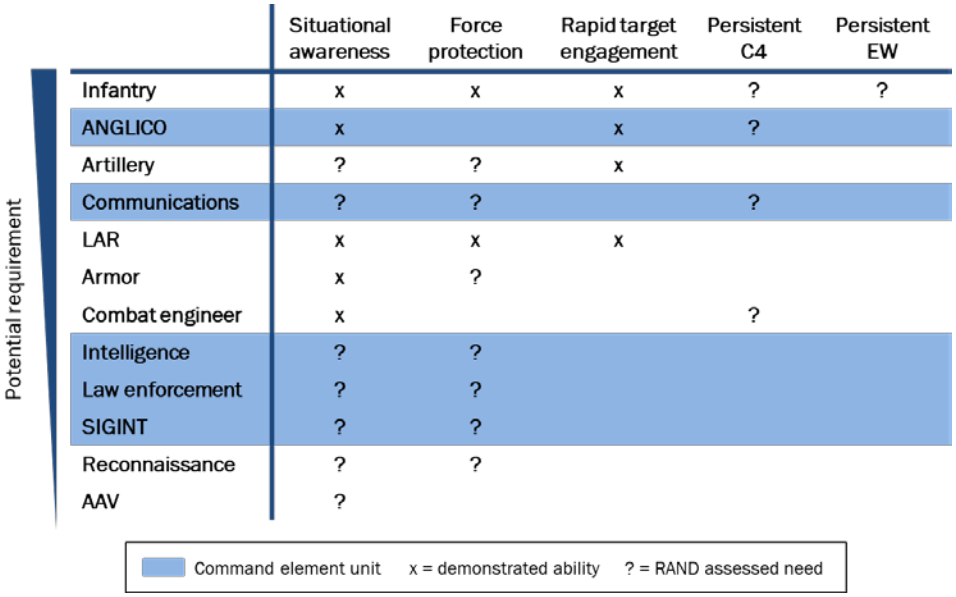
> We call for fire with the Ravens and Pumas regularly. … We’ve done multiple exercises with the mortars organic to the company and artillery. Both have been used and we’ve adjusted fire off both of them.

At the same time, our interactions with artillery units—units who would be an obvious beneficiary of SUAS-enabled rapid target engagement—suggested less consistent usage. When contacted, some artillery units claimed that they did not use SUAS in any capacity at all. Others discussed using SUAS only for situational awareness. A division SUAS program manager observed:

> Artillery units don’t use it as much as you’d think. I was surprised that they don’t use them more. For targeting, [battle damage assessment], from division perspective [this would be useful] especially during exercises.

There were even fewer mentions of persistent EW (four mentions in four interviews) and persistent C4 (three mentions in three interviews) by SUAS users. As a whole, interviewee responses indicate that experience across the five mission profiles is uneven. Situational awareness and force protection uses are understood, rapid target engagement uses are somewhat understood, while other mission profiles are far less so.

This is not to say that all OccFlds require the same level of proficiency across all the SUAS mission profiles. From interview responses and the literature review, we formed a hypothesis that different communities have varying needs for these mission profiles. Our research shows that the infantry community has a clear need for all five mission profiles, but it is not yet clear which mission profiles are crucial for others. Figure 3 provides our current assessment of which mission profiles might be required for each community.


Potential requirement

	Situational awareness	Force protection	Rapid target engagement	Persistent C4	Persistent EW
Infantry	x	x	x	?	?
ANGLICO	x		x	?	
Artillery	?	?	x		
Communications	?	?		?	
LAR	x	x	x		
Armor	x	?			
Combat engineer	x			?	
Intelligence	?	?			
Law enforcement	?	?			
SIGINT	?	?			
Reconnaissance	?	?			
AAV	?				

▨ Command element unit x = demonstrated ability ? = RAND assessed need

Figure 3. **RAND-Assessed Potential Mission Demand by Unit Type**

Note. Source: RAND analysis

We believe the Marine Corps should consider identifying each OccFld/unit's true demand for each mission profile. This will be a crucial task that will shape requirements across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) and help the Marine Corps take the fullest advantage of SUAS at the least risk of making a poor investment decision.

Access Is Key to Further Understanding of SUAS Utility

We found that the infantry and LAR communities had the most mature understanding of SUAS. For the infantry, this is because it has been given priority in accessing platforms. A MEF SUAS program manager (PM) illustrated this:

> So what I base everything off of is the [SUAS] fielding plan, so we're keeping that going as a good place to start. It's a good baseline, but the problem is there are so many other units and there's not enough inventory to go across the spectrum. … For example, units A and B went out the door with almost three times the systems because their [concept of operation] was briefed to Commandant [of the Marine Corps]. [We] have to balance

> the small number of systems across the [MEF]. If you don't have anything going on, I'll probably take your systems.

Because the infantry has such extensive exposure to the platforms, the infantry had the opportunity to develop and refine CONEMPs for situational awareness, force protection, and (to a lesser extent) rapid target engagement. We also observed that the infantry has started to consider the potential utility of SUAS for providing persistent C4 and EW.

The LAR community gained its understanding of SUAS differently. Rather than gaining exposure through prolonged access to existing platforms alone, some of its units also have direct access to the Marine Corps Warfighting Lab (MCWL), the Office of Naval Research (ONR), and through them, SUAS contractor teams. Through those organizations, the LAR community has been able to focus directly on experimenting with CONEMPs and with different platforms instead of learning through exposure alone. Because of this different form of access and the relatively small size of the LAR community, it has achieved a level of SUAS maturity that is comparable to that of the infantry. However, we do not believe the LAR community approach is scalable because direct relationships with the MCWL and ONR can only be sustained for a small number of units.

The other communities had lower levels of experience using the platforms in training and during deployment. Interview responses and AAR reviews suggest that most communities have had some access to SUAS, but such access has not been consistent. In some cases, units were not aware they had access to the platforms, despite the fact that such platforms were on their unit tables of equipment (T/Es). We believe the way that the Marine Corps has prioritized SUAS access over time has suppressed demand from low-priority units. In other words, these units have learned to stop requesting SUAS. One battalion commander's observation highlights an extreme case:

> I was six months into job before I knew we had designated [RQ-20B] Pumas. It was just a drive by conversation. I saw sheet of paper. There is education gap between what [HQMC and higher echelons] produce and the information they disseminate to units. Some units still don't know they have airframes designated for them up there.

When units do gain access to SUAS, they often must focus on maintaining operator currency on the platforms—activities that contribute little to a unit's ability to employ SUAS as described in the mission profiles or to support any other unit task. One SUAS PM from a low-priority unit observed that maintaining operator currency (discussed more later) is his key concern.

> The main thing with SUAS is that they need to be more available. So currency prevents them from being used because it's impossible to be current. I would like to use them more, but it takes a [lot] of work to be current.

As a result of uneven access, units across the CE and GCE have uneven experience employing SUAS. Units that have sufficient access to SUAS have room to experiment with CONEMPs, gain experience with SUAS, and determine the true demand for SUAS. Units that have little access are only able to sustain basic operator skills to maintain currency. We also observed differences in SUAS experience across different units of the same community. This was particularly evident in our interactions with the artillery community. Consistent access drives understanding of how SUAS and SUAS mission profiles contribute to a community.

Non-Material Issues Must Also Be Addressed to Increase Access

We also found that significant impediments to greater SUAS maturity in the Marine Corps are not related to material solutions. Although our protocols focused mainly on material topics, a consistent trend in user interviews was a focus on non-material issues. The most cited issues were doctrinal, personnel, and training, each of which is described next. Although non-material aspects of SUAS employment were out of the scope of this research, the issues described next are relevant to the issue of SUAS access previously discussed. Further research should be conducted into the full range of DOTMLPF issues impacting the use of SUAS by CE and GCE units and how they might be addressed.

Lack of Agreed-Upon SUAS Doctrine and Concepts Impedes Tactical-Level Usage

The Marine Corps today lacks SUAS doctrine and concepts of employment for CE and GCE units. Some service-wide guidance has been articulated, but such guidance is insufficiently detailed. Guidance includes a reference publication on unmanned aircraft systems (MCRP 3-20.5, *Unmanned Aircraft System Operations*) and the SUAS training and readiness (T&R) manual (NAVMC 3500.107). MCRP 3-20.5 contains useful employment information and considerations but is meant primarily for Group 3 platforms employed by dedicated unmanned aircraft squadrons. The T&R manual provides standards for training Group 1 operators, but it offers nothing on employing SUAS operationally.

The lack of generally understood doctrine, CONEMPs, and other service-wide direction impedes the general utility of SUAS. We observed from our interviews that many units can conceptualize the situational awareness and, to lesser degrees, force protection and rapid target engagement profiles without doctrine or other guidance. However, few interviewees could imagine the utility of SUAS for persistent C4 and persistent EW. Without a basic understanding of these profiles, units cannot determine the true need for SUAS in their units. Furthermore, the lack of doctrine or other guidance impedes consistent understanding of the required training and support needed to allow units to fully use SUAS.

Personnel Management Is Inefficient and Can Affect SUAS Operations

Another issue that impedes SUAS maturity across the CE and GCE is the uneven availability of qualified operators. SUAS training is not centrally tracked in the Marine Corps, thus making it difficult to manage the Marine Corps' inventory of trained operators. This can make it difficult for a unit to ensure that it has enough current, qualified operators to support its mission. For example, several units reported difficulty in maintaining visibility into its SUAS operators' currency. Units also lose SUAS operators due to normal personnel rotations and are sometimes unable to secure other training opportunities in time to support a deployment.[13] This concern is exacerbated by the TALSAs' relatively limited training capacity and the relatively small number of operators already trained; rectifying a training shortage within a reasonable timeframe may not be feasible for some units. Finally, the need for effective SUAS personnel management will only grow as the Marine Corps reorganizes itself to more fully integrate SUAS and other technologies into its operations.

Training

We observed two training-related issues that negatively impact SUAS maturity across the CE and GCE. First, formal SUAS training (provided by the TALSAs) is focused

[13] User interview

on system basics and does not provide instruction on how to employ SUAS operationally. The remarks of one unit's SUAS program manager are typical:

> My lance corporal had good enough training to operate, but he lacked the tactical aspect. Our biggest problem with SUAS is a massive gap between learning how to fly it and then how to use it tactically. The lance corporal gets to fly for half an hour one time a month. I'm here to bridge the gap and teach him how to find things through a sensor. What we don't have is some type of institution that will standardize this training and bring lance corporals from being able to operate it, [to] fly[ing] it tactically.

Second, current training areas may be insufficient to support all SUAS mission profiles. One of the biggest limiting factors is access to ranges where units can fly SUAS. Range control regulations at some bases limit units' abilities to train effectively. For instance, Camp Lejeune–based units are not allowed to conduct SUAS handoffs without both pilots having visual contact with the platform.[14] Also, units are not allowed to operate from a moving platform (e.g., HMMWV, LAV, etc.), although doing so is critical to exploiting SUAS in an operational environment. Current range restrictions may require units to spend extra time and resources to get exceptions, or such restrictions may not be waived at all. This prevents units from incorporating SUAS more fully into individual and collective training.

Three Procurement and Allocation Models Address the Access Need to Varying Degrees

From our mathematical matching and quantity identification process, we articulated two different allocation models based on different parameters we identified as essential and compared them to the Marine Corps' status quo model. These alternatives helped us demonstrate what factors were drivers of cost and capability for investment in SUAS technology. The three models were

- a **status quo** model that is based heavily on current Marine Corps procurement strategies
- an **economy buy** model based on the full buy option that economizes by reducing access (and thus, total platform quantities) to platforms during some periods of a unit's deployment cycle
- a **full buy** model developed from our analysis that meets all identified strategic procurement and allocation goals

Representative unit costs were used for all models and are shown in Table 3. Recommendations are shown in Table 4.

Table 3. Representative Unit Costs

EOTACS category	Example Platform	Representative Unit Cost
2 (Nano/VTOL)	PD-100	$51,000
3 (Micro/VTOL)	Instant Eye	$18,000
4 (SR/SE VTOL)	SkyRanger	$200,000
5 (SR/SE FW)	Wasp, Raven	$293,500*
6 (MR/ME FW)	Puma	$267,000
7 (LR/LE FW)	Stalker XE	$1,547,770

[14] User interview

Note. *Cost figure is an average of Raven and Wasp unit costs

** Only direct material costs for example platforms are shown here. Costs are meant to be strictly representative; decision-making based on these costs should consider updated cost information or assumptions.

Source: RAND and HQMC(CD&I) analysis

Table 4. Representative CE and GCE SUAS Procurement and Allocation Recommendations to FY2025 by Occupational Field

	Status Quo		**Economy Buy**		**Full Buy**	
	Quantity*	**Cost ($m)**	**Quantity***	**Cost ($m)**	**Quantity***	**Cost ($m)**
Infantry	1,676	160	2,434	274	2,634	289
ANGLICO	30	8	12	11	36	31
Artillery	30	8	63	45	108	65
Communications	0	0	17	5	21	6
LAR	20	6	282	86	322	96
Armor	19	5	29	45	42	65
Combat engineer	26	7	85	17	129	26
Intelligence	7	2	9	2	12	2
Law enforcement	0	0	26	5	39	8
SIGINT	6	2	3	5	6	9
Reconnaissance	26	7	159	6	237	9
AAV	0	0	23	6	33	9
Total	**1,840**	**205**	**3,142**	**506**	**3,619**	**616**

Note. * Combined total of all Category 2-7 platforms

Source: RAND and HQMC(CD&I) analysis

Status Quo

The status quo option was developed by HQMC(CD&I) prior to this research. This option expands the current SUAS inventory somewhat; it mainly procures more RQ-20B Puma platforms in response to some unit-level inputs but does not take the divestiture of Category 5 (SR/SE fixed wing) RQ-12A Wasp and RQ-11B Raven platforms into account. It preserves the current focus on infantry units. No Category 7 (LR/LE fixed wing) platforms are identified. No platforms are identified for assault amphibian, law enforcement, or communications units. It represents 50% of the full buy quantity developed from this analysis.

Economy Buy

The economy buy option provides similar expected platform availability to all OccFlds and echelons as the full buy option, but at reduced cost. In this option, active component infantry and light armored reconnaissance (LAR) units manage their SUAS inventories organically. Centralized training and logistics support agencies (TALSAs) continue to manage non-infantry and LAR unit inventories. Quantities are reduced to two-thirds of the full buy to account for typical force generation for typical unit deployment rotations; this makes platforms available to units undergoing pre-deployment training and deployment cycles, but not during their post-deployment recovery phase.[15] This cut 732 platforms across all categories from the full buy option and saves $78.25 million in direct material costs.

Full Buy

The full buy option fulfills our predicted demand and procures enough platforms to ensure availability for all units at any stage of the unit's training and deployment cycle. TALSAs continue to manage non-infantry and LAR unit inventories.

Findings and Recommendations

The Marine Corps has made significant advances in developing its SUAS proficiency since 2015, when its current goals were articulated. Still, there is more potential in SUAS that the Marine Corps has not fully exploited. Separately, SUAS technology is advancing to meet commercial, as well as military, needs. This is an unusual confluence of circumstances that DoD and Marine Corps force development processes were not designed to accommodate. In that light, we offer the following recommendations to best leverage this emerging technology:

- *Invest significantly more (on the order of $500 million) over the next five to six years to redouble experimentation and conceptual development efforts.* We recommend an investment strategy that prioritizes procurement of capabilities for infantry and LAR communities to help them further integrate SUAS into their operations and allows all other CE and GCE communities to explore the full range of utility that SUAS may provide. To enable that effort, procurement approaches should balance three elements: maximizing capability, minimizing technological regret, and minimizing cost.
- *Conduct further analysis into demand and usage to enable tailored procurement approaches.* Further analysis is required of each of OccFld's true demands for SUAS in each of five identified mission profiles. Additionally, the Marine Corps should facilitate the collection of more precise usage data, and analysis of SUAS market dynamics are needed to support SUAS investment decisions that can keep up with the technology's fast development pace.
- *Research full range of DOTMLPF issues.* Our analysis found that significant impediments to greater SUAS maturity in the Marine Corps are not related to material solutions. Further analysis of DOTMLPF considerations is required. We recommend that the Marine Corps review and refine its SUAS doctrine, manpower management, and training to fully cement operational insights and best practices already found.

SUAS technology has significant potential to contribute to the force described in the Marine Operating Concept. However, this technology's fast development unrelated to U.S. military needs demands a force development approach that relies heavily on fast iterative operational experimentation and conceptual development. Our assessment of previous

[15] This assumption is derived from typical deployment cycles and global force management processes; this ratio can be changed depending on substantive changes to these guiding principles. This economization was inspired by the example of MEU explosive ordnance disposal (EOD) equipment set sharing practices; only enough equipment is procured to outfit units training for deployment and currently deployed, but not those recovering from deployment.

Marine Corps SUAS investment decisions indicates that they were mindful of this; our recommendations provide a means to continue that approach as the Marine Corps scales up its SUAS investments.

References

Dalby, J. A. (2013). Puma: A company-level ISR solution to expeditionary operations. *Marine Corps Gazette, 97*(8).

De Vries, H., Elliott, M. N., Kanouse, D. E., & Teleki, S. S. (2008). Using pooled kappa to summarize interrater agreement across many items. *Field Methods, 20*(3), 272–282.

Gillis, J. (2017). In over their heads: U.S. ground forces are dangerously unprepared for enemy drones. Retrieved from https://warontherocks.com/2017/05/in-over-their-heads-u-s-ground-forces-are-dangerously-unprepared-for-enemy-drones/

NCOs, SNCOs, & Officers of 3d Bn 5th Marines. (2017). Sea dragon 2025: Small unit leaders' thoughts. *Marine Corps Gazette, 101*(8).

Satty, T. L. (1986). Axiomatic foundation of the analytic hierarchy process. *Management Science, 32*(7).

Turnbull, G. (2019, February 19). The Navy plans to test its new electronic warfare drones this fall. *C4ISR Net*.

U.S. Marine Corps. (2016). *Marine operating concept: How an expeditionary force operates in the 21st century*. Retrieved from https://www.mccdc.marines.mil/Portals/172/Docs/MCCDC/young/MCCDC-YH/document/final/Marine%20Corps%20Operating%20Concept%20Sept%202016.pdf?ver=2016-09-28-083439-483.

U.S. Special Operations Command. (2018). Request for information (RFI) for expeditionary organic tactical airborne intelligence, surveillance and reconnaissance (AISR) capability set (EOTACS) of small unmanned aircraft systems (SUAS).

Acknowledgements

The authors wish to acknowledge the considerable assistance provided by our DoD sponsors who commissioned this research, Maj Clayton Jarolimek, Maj Chase Thompson, and Capt Shelby Ochs. We also thank our government study leads, Capt Elle Ekman and Robert Hayden of the Marine Corps' Operations Analysis Directorate.

We are also grateful to the other members of the study advisory committee and other stakeholders for their input, guidance, and introductions, including Col Charles McLean, LtCol James Lively, LtCol Sean "Husker" Merlin, Ernie Cardenas, Doug Doerr, Jon "Blade" Hackett, Kevin McConnell, and Air Force Lt Col David "Mudd" Willard. We also thank the 69 interviewees who provided invaluable insights on SUAS for this research.

We thank our RAND colleagues Paul DeLuca, Mike Decker, and Igor Mikolic-Torreira (our dedicated reviewer) for providing helpful advice and feedback on this research. We also thank Ben FitzGerald for his thoughtful review comments. Jia Xu and Colin Ludwig provided early insights as we framed the problem. Elizabeth Hastings-Roer, Ben Goirgolzarri, Lindsey Polley, and Russell Williams contributed to the analyses. Felix Knutson and Kurt Klein assisted with notetaking. Their efforts improved the quality of this research.

Technology Trust: The Impact of Trust Metrics on the Adoption of Autonomous Systems Used in High Risk Applications

Michael Anderson—is a PhD student at the Naval Postgraduate School, Monterey, CA.

Johnathan Mun—PhD, is a Research Professor at the Naval Postgraduate School, Monterey, CA. [jcmun@nps.edu]

Abstract

As autonomous systems become more capable, end users must make decisions about how and when to deploy such technology. The use and adoption of a technology to replace a human actor depends on its ability to perform a desired task and on the user's experience-based trust that it will do so. The development of experience-based trust in autonomous systems is expensive and high-risk. This work focuses on identifying a methodology for technology discovery that reduces the need for experience-based trust and contributes to increased adoption of autonomous systems. Initial research reveals two problems associated with the adoption of high-risk technologies: (1) end user refusal to accept new systems without high levels of initial trust and (2) lost or uncollected experience-based trust data. The main research hypothesis is that a trust score, or trust metric, can influence the initial formation of trust by functioning as a surrogate for experience-based trust, and that trust in technology can be measured through an odds-based prediction of risk.

Introduction

> We had better be quite sure that the purpose put into the machine is the purpose which we desire.
>
> —Norbert Wiener, 1960

The use of technology by the Department of Defense (DoD) depends on its ability to perform a desired task. There are many issues associated with trust in technology that are increasing in importance as the U.S. military begins to acquire and deploy autonomous systems. In order to ensure the effective adoption of new innovations in technology, there is a need to establish a system of metrics that justify a level of technology trust. This proposed research has the explicit goal of investigating and recommending trust metrics by applying advanced analytical methodologies to increase the speed and effectiveness of the adoption of new technologies. This investigation proceeds by participating in an evaluation of technologies for use in evolving high-risk military applications. The trust metrics are measured in terms of the technology acceptance versus system control.

Technology Trust

Devitt (2018) implies that in order to meet the DoD requirements for increased speed of adoption for new technologies, there is a need to replace the model of developing trust over longer periods of time with a justifiable metric of trust. This research studies the effectiveness of establishing and introducing trust metrics on the evaluation and selection of technologies. The work participates in an ongoing assessment of autonomous systems for use in high-risk military applications throughout fiscal year 2019. A model is developed that optimizes the cognitive impacts of these trust metrics as they relate to the technology selection and adoption process. The approach will be extensible and can be adopted into private industry.

Research Problem

The recent increase in the use and deployment of commercial technologies by other countries is a disruptive threat to the United States' technological superiority. The rapidly changing technology landscape requires DoD laboratories to increase the speed at which they adopt new technologies (David & Nielsen, 2016). With declining budgets in research, it is imperative that the DoD establish new methods for rapidly adopting and effectively deploying new and emerging technologies whenever possible.

Research Purpose

As autonomous systems begin to surpass the capabilities of humans, there is a need to establish a level of confidence in a technology's ability to perform as expected. The complexity of modern systems makes it difficult to establish a comprehensive metric of trust. Past research in technology trust focused on automation and methods to measure interpersonal person-to-firm relations, such as trust in a Web vendor or a virtual team member (McKnight et al., 2011). This research has the goal of establishing and measuring a comprehensive trust metric for individual pieces of technologies, such as autonomous systems, used in high-risk military applications. The development of a trust metric serves two purposes: first as a surrogate for experience-based trust by contributing to the formation of initial-trust and, second, as a collection tool for capturing experience-based trust data.

Research into a "trust-discovery" methodology contributes to improved understanding of human-machine trust formation and the development of a technology-literate workforce capable of accurately assessing new technology for a given operational scenario. This work first establishes a baseline definition of what it means to "trust" technology. It concludes with the development of a methodology leading to trusting relations between humans and technology. This work contributes to the literature in areas of trust in autonomous systems, technology adoption, and technologies intended for use in high-risk applications where failure or improper application can lead to severe consequences.

Research Questions

This study attempts to answer the following questions:

1. How do varying levels of system control affect the development of trust in technologies used in high-risk military applications? The constructs researched include
    a. Perceived ease of use
    b. Perceived usefulness
    c. Intent to use
2. How do anthropomorphic metrics affect the development of trust in technologies used in high-risk military applications? The constructs researched include
    a. Hardware
    b. Algorithms
    c. Links

Research Approach

The following research approach is used:

1. Study the evaluation process of autonomous systems for use in high-risk military applications.

2. Develop a conceptual framework for trust metrics that optimizes the technology evaluation process.
3. Observe and record the results of both laboratory and field experimentation.

The basic tenets of the experimental design are realized through a 2 x 3 factorial design (Table 1).

Table 1. 2 x 3 Factorial Design

		SYSTEM CONTROL		
		LOW	MID	HIGH
TRUST METRIC	NOT USED	…	…	…
	USED	…	…	…

Contribution

The concept of a technology trust metric has applicability beyond the DoD. Private industry can greatly benefit from the concepts and methodologies developed in this research by applying trust metrics to the research and development of existing or new consumer technologies such as machine learning (ML), artificial intelligence (AI) systems, smart algorithms, and embedded technologies. These intelligent systems are transformative areas that will eventually integrate into all industries (e.g., self-driving cars, delivery drones, big data analytics, and the Internet of Things, where algorithms, machines, and computer systems are continually learning and evolving).

This research also contributes to trust theory and provides an increased understanding of military technology acceptance. The recommendations provide a conceptual framework for how a military community develops trust in technologies for high-risk missions and how varying factors influence the development of such a relationship. Currently, there is an effort within the DoD to perform such trust analytics, an effort in which this current research will participate.

Organization

Literature Review section: This review investigates existing literature that includes terms such as *technology trust and risk, decision making,* and *technology-adoption models*. A review of current and past theory on technology trust and decision making is developed in the Literature Review, which is then used to develop a comprehensive metric for assessing technology trust within the DoD. A proposed framework for a comprehensive trust metric is identified and introduced to the technology evaluation process.

Experimental Design section: Both lab and field experiments are conducted to identify trust metrics. This research intends to leverage an ongoing DoD experiment reviewing and selecting a series of new autonomous systems. The existing data is collected from DoD active duty technology end users as well as civilian scientist support staff. The study investigates how varying levels of trust influence cognitive decision making as well as technology adoption. The primary product of this investigation is the experimental data obtained.

Literature Review

The purpose of this section is to understand the formation of trust as well as analyze the constructs of a trust relationship. The idea of trust metrics is broken down into quantifiable sections based on leading theories. We conclude by presenting a conceptual framework for a technology trust metric based on what was learned from the literature as well as what is missing from the literature.

This research was initiated through informal interviews that attempted to identify the factors that contribute to the use of technology in high-risk environments. The participants were a small group of active-duty military and veterans that deploy, or have deployed, with technology that posed great risk of physical harm should it fail. A number in this group experienced significant injury due to the failure of technology, and the potential for bias was noted. The open-ended questions were based on what the users did or did not like about using technology in high-risk scenarios. The initial coding of interviews revealed the following themes:

1. Hands-on experience with technology is critical for establishing trust, and team-based reputation for a technology is as important as personal experience.
2. Users favor simple technology containing only the features needed to accomplish a mission, and users reject new technology in favor of older and more trusted systems.
3. Personal investment in a mission is key to learning how to use new technology.

These themes all have implications for the adoption of autonomous systems within the DoD. Advanced robotic systems have the ability to improve performance in a number of military roles while reducing risk to humans, and it is important to understand how to improve the adoption of such systems within the DoD. This initial research focused on technology in dangerous environments and reveals that adoption is highly dependent on the ability of the user to obtain the knowledge necessary to develop trust. This theme led to our initial literature review on understanding trust and how it applies to technology adoption.

The literature review was developed through searches on both Web of Science and Google Scholar using combinations of search terms such as *trust, knowledge-trust, technology trust, human-computer, human-robot, technology acceptance, trust attribute, trust risk, and risk score*. The literature results were narrowed to 93 relevant articles.

Knowledge

The process of obtaining knowledge is fundamental to the establishment of trust. We therefore briefly review the epistemologies, or the processes for how a person gets to know something, as concepts important to this work. Early philosophers presented the two opposing views of the source of knowledge: rationalism or empiricism.

The French philosopher Rene Descartes was an early rationalist who believed that we can only know something through reason, and that the only thing we can truly know is that we have consciousness. Descartes presented a methodology for knowing what is real that rejects a construct needed for the establishment of technology trust. He established a dualism that reduces our understanding to distinct areas of consciousness and matter but does not account for the senses. Our sense perception, he believed, is easily prone to error due to subjective interpretation. He believed that the senses are meant to simply get us around in the world rather than lead us to truth. In order to test our hypothesis of trust in technology, we must identify constructs that permit measurement of human interaction with technology, and technology interaction with its surroundings.

John Locke later introduced empiricism, which, contrary to rationalism, stated that all knowledge must be obtained through experience. The empiricists claimed that the senses were the only way to true knowledge, and that experience is much more accurate than anything the mind could ever reproduce through memory or reason. The theories presented by rationalism and empiricism both stand to contribute to the formation of trust through the application of reason-based knowledge and experience-based knowledge. (However, there is a limitation in that we lack a method for integrating these two forms of obtaining knowledge.)

Further review reveals that modern philosophers reject the idea that knowledge is obtained exclusively through either rationalism or empiricism. The philosopher Immanuel Kant provided a synthesis between the two opposing theories. First, he noted that reason lacks the ability to create sensory experience; it is only through reason that we are able to accurately analyze the stimuli received through the senses. This theory represents a foundation for understanding the development of trust. Figure 1 represents a causal model based on our finding in literature that includes a synthesizing feedback loop to represent how we come to know something.

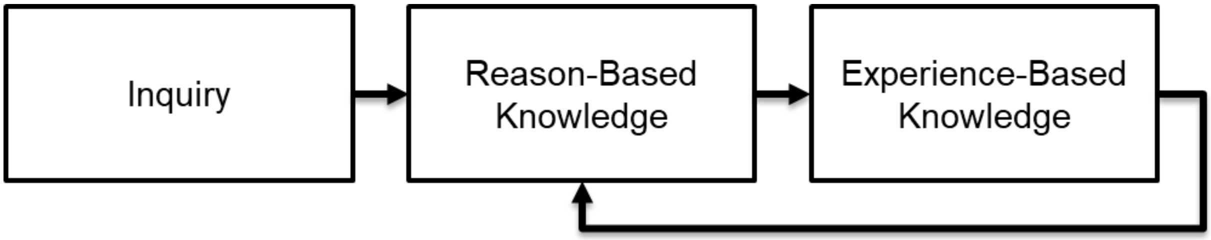


Figure 1. **A Model of Inquiry Leading to Knowledge**

Trust

Castelfranchi and Falcone (2010) review over 72 definitions of what it means to know something well enough to have trust, and their work reveals a great deal of confusion and ambiguity surrounding the use of the term. The concept of trust appears to be subjective in nature, and the literature does not provide a commonly accepted definition across research disciplines. Agreement in the literature was found for the definition of trust in two small areas: (1) the basic premise of trust involves two actors, and (2) trust is a relationship in which one entity relies on someone, or something, based on a given criterion. Research into the meaning of a “given criterion” reveals an interchangeable use of the terms *trust* and *confidence*. The only noticeable difference in the use of these terms is that trust is based on decisions involving risk, whereas confidence involves decisions devoid of consequence.

This literature review furthers its investigation into trust through researching interpersonal relationships. Leading theories on interpersonal trust present vulnerability and risk as the contributing factors unique to the development of such a relationship. Cho, Chan, and Adali (2015) surveyed the meaning of trust across academic disciplines and identified that it follows a basic premise involving risk. For example, they found that in psychology, academic researchers of trust assess the probability that individual behaviors are repeatable in situations that entail risk, and in sociology, researchers of trust assess the probability that one party will perform an action that will not hurt the interests of a dependent party or expose them to risk due to ignorance or uncertainty.

Rousseau et al. (1998) define interpersonal trust as a psychological state of a trustor accepting vulnerability in a situation involving risk, based on positive expectations of the intentions or behavior of the trustee. Boon et al. (1991) simplify the definition of trust as a state involving confident predictions about another's motives in situations entailing risk. The majority of early research on trust involves person-person relationships and provides a starting point for our understanding of the process of developing trust. Figure 2 presents an operational model of interpersonal trust formation based on reviewed literature.

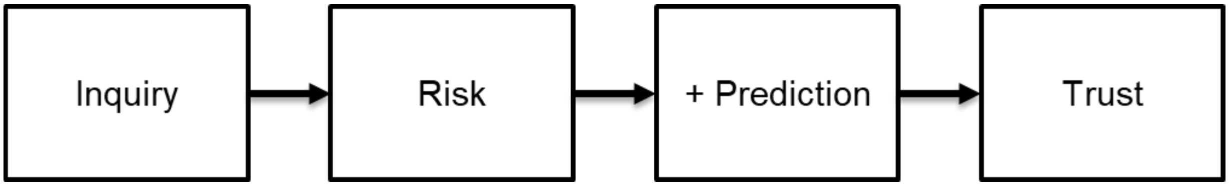


Figure 2. **A Model of Interpersonal Trust Formation**

Adams and Webb (2002) describe two broad processes of developing trust between two individuals. The first is defined as "person-based trust," which develops through repeated engagements, and the second is called "category-based trust," which develops in the absence of direct experience. These definitions parallel the theories identified in our previous research into the epistemologies. Consequently, we modify interpersonal trust terminology to match our research by replacing "category-based" with "reason-based" and "person-based" with "experience-based."

Kramer and Tyler (1996) assess reason-based trust and present it as useful for understanding how one develops a trusting relationship when personal or social interaction is not possible. This type of trust often develops through someone's membership in a familiar group or category. The factors contributing to reason-based trust can be social roles, training, or experience. In reason-based trust, the relationship is most commonly developed through a reputation that serves as a proxy for personalized knowledge and direct experience. These concepts lead to our first research hypothesis regarding the experience-based trust relationships.

H1: An experience-based proxy will influence the tendency to trust or distrust.

Rempel, Holmes, and Zanna (1985) assess that experience-based trust relationships develop over a long period of time through personal interaction. In their early research on trust, they describe three factors that influence the development of trust as competence, benevolence, and integrity. Their work also discusses the significance of the mental motivation behind the desires to establish a relationship and found it was strongly correlated to the factors that influence trust. Their work confirms a theme identified in our early interviews with users of technology in risk-application that emphasized the importance of personal investment. It also leads to our second hypothesis relating motivation to technology acceptance.

H2: Increased personal motivation will increase technology acceptance.

There appears to be general agreement in the literature reviewed that interpersonal trust consists of two categories: first, that trust is both reason-based and experience-based, and second, the strength of the trust bonds may differ. The concept of initial trust involves the development of a relationship based purely on reason and represents a weaker connection that can be explained by first impressions. The second category of experience-based trust involves direct knowledge and regular interaction. This type of trust represents a stronger connection and is explained by relationships that develop over a longer period of time through an experience-reason feedback loop. Figure 3 presents a model of interpersonal trust.

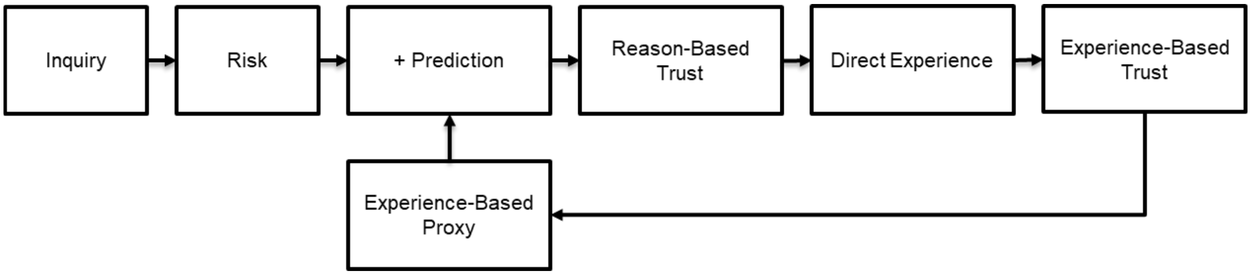


Figure 3. **Interpersonal Trust Lifecycle**

Technology

The past research on interpersonal trust applies in many ways to trust in technology. This study sought out literature that contributes to the development of a methodology of technology discovery leading to person-technology trust. The potential for integrating interpersonal trust research into technology trust was discussed by McKnight et al. (2011). This research found that interpersonal trust is based on a trustee's expectations and reliance on a trustor to perform as expected through benevolence, even though the trustor possesses the volition to choose to do what is right or what is wrong. Since technology does not possess volition (ability to choose), some researchers went as far as to dismiss the idea of trust in technology as irrelevant. However, recent advances in artificial intelligence refute the claims that technology lacks volition. This is confirmed in the vast amount of current research into how autonomous systems make decisions that can either harm or protect human life.

Technology trust research is further represented in multiple disciplines of engineering and science. The major fields of technology trust research include, but are not limited to, artificial intelligence, command and control, human-computer interaction (HCI), data fusion, human-machine fusion, cyber security, and automation. Multiple models for researching trust that combine both human-like and system-like terminology are presented in the literature. Technology trust is a multifaceted area of research that integrates both human-like measures and system-like measures. Three of the most frequently used human-like terms used to model technology are *competence, benevolence,* and *integrity*. The work by McKnight et al. (2011) and Lankton, McKnight, and Tripp (2015) consider the system-like alternate terms for technology trust as *reliability, functionality,* and *helpfulness*. A number of system-like measures of technology trust were identified that are outside the scope of this work but still important to ongoing trust research. These potential system-like measures include supply chain management, past vendor performance, hardware/software-oriented security, and network security.

The majority of the language used to describe interpersonal trust can apply to technology trust. For example, the word *benevolence* is a very human-like attribute that is likely to appear in future literature on the decision-making capabilities of self-driving cars. A total of 86 factors and attributes related to interpersonal and technology trust were collected from the literature to form a random nomological network of trust terms. A *factor* is described as situational consideration of technology use that has the potential to influence trust, such as risk and time to operate. An *attribute* is a characteristic inherent to the technology such as its speed, power, and processing capability. The combined and unsorted list is presented in Table 2. Future experimentation involves understanding the influence of these terms in the following areas:

1. Factors that measure reason-based and experience-based technology trust
2. Attributes that characterize technology trust as a proxy for experience

Table 2. Nomological Network of Trust Factors and Attributes
(Cho et al., 2015; DeVitt, 2018; Hoff & Bashir, 2015; McKnight et al., 2011; Schaefer, 2016)

Ability	Character	Disappointment	Importance	Process	Skills
Adaptive	Communication	Disposition	Incompetent	Protect	Stability
Adoption	Competence	Dynamic	Integrity	Purpose	Supportive
Adversarial	Completeness	Easy	Intelligibility	Rationality	Teammate
Altruism	Confidence	Expectation	Intent	Recency	Trainable
Attractive	Contract	Experience	Knowledge	Reciprocation	Transparency
Autonomous	Control	Faith	Learning	Regret	Uncertain
Availability	Cooperation	Faults	Likeable	Relational	Understandability
Awareness	Credibility	Fear	Monitored	Relevance	Unstructured
Belief	Credit	Feeling	Motives	Reliability	Utility
Benevolence	Decisive	Frequency	Perception	Relief	Validity
Capability	Delegation	Frustration	Performance	Responsive	
Capital	Dependability	Helpfulness	Popular	Risk	
Centrality	Difficult	Honesty	Power	Robust	
Certainty	Directability	Hope	Predictability	Similarity	

Figure 4 represents the integration of technology trust with the interpersonal trust factors and attributes included in our nomological network of terms.

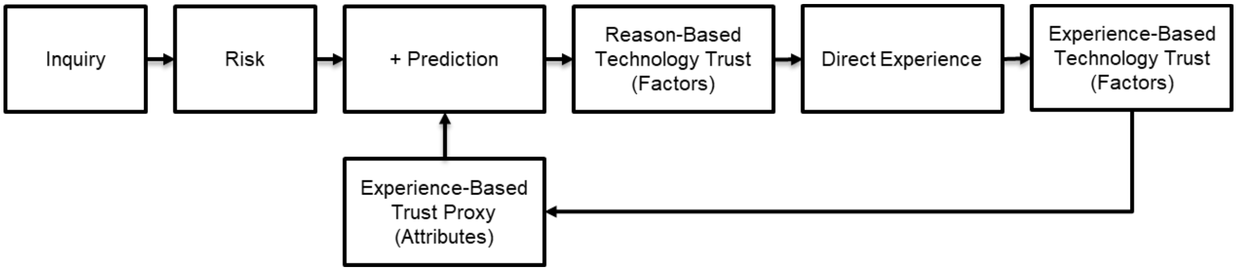

Inquiry
Risk
+ Prediction
Reason-Based Technology Trust (Factors)
Direct Experience
Experience-Based Technology Trust (Factors)
Experience-Based Trust Proxy (Attributes)

Figure 4. **Technology Trust Lifecycle**

A theory relevant to measuring and characterizing trust is found in the technology acceptance model (TAM) developed by Fred Davis nearly 30 years ago. This model plays a significant role in the majority of research investigating the factors and attributes that influence the acceptance of a technology. Venkatesh and Bala (2008) present the TAM's ability to predict individual adoption and use of technology. The TAM assesses the behavioral intention to use a technology through two constructs: perceived usefulness (PU), which is defined as the extent to which a person believes that using a technology will enhance his or her job performance, and perceived ease of use (PEOU), which is defined as the degree to which a person believes that using a technology will be free of effort. These two variables are used to establish a relationship between external influences and potential system usage (Gefen, Karahanna, & Straub, 2003). In the work by McKnight, Choudhury, and Kacmar (2002), it was experimentally determined that the TAM variables do not predict continued use of a technology outside of initial acceptance and that trust in a vendor's past technology does not translate to acceptance of subsequent technologies.

Tétard and Collan (2009) address the challenges of adopting new technology in their work on the lazy-user theory. This theory states that a user will select the technology that demands the least amount of effort to do the job. This theory also addresses one of the themes identified in our early grounded theory study interviewing operators of technology in high-risk scenarios. The application of this theory places technology users at a disadvantage, particularly in high-risk military applications where trustors are known to avoid more capable technology for systems that are easier to understand. If an experience-based proxy can improve the accuracy of developing trust through increased technology literacy, it may lead to increased acceptance of more complex and capable technologies, thereby reducing the influence of the lazy-user theory. This leads to our third research hypothesis.

H3: An experience-based proxy will decrease the influence of the lazy-user theory on technology acceptance.

Conclusions

The intent of this section is to identify gaps in research on trust in autonomous systems. It appears that a methodology of technology discovery that leads to trust is not available. This review reveals a clear distinction between reason-based trust and experience-based trust. It also suggests that users are willing to trust technology in high-risk environments and that an experience-based proxy may increase the quality of such a relationship and the pace at which it is established. Based on the finding in literature, Figure 5 illustrates a conceptual framework for a causal methodology of technology adoption by introducing an experience-based proxy that is hypothesized to improve technology adoption. The impact of a proxy introducing inaccurate information is noted as significant but is outside the scope of this work.

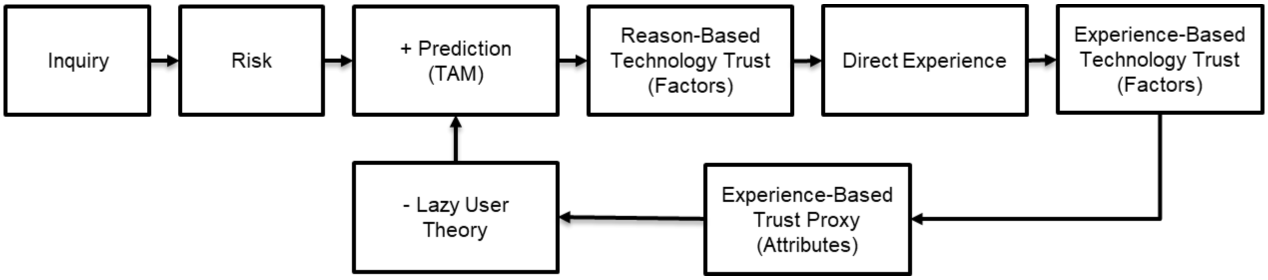

Inquiry
Risk
+ Prediction (TAM)
Reason-Based Technology Trust (Factors)
Direct Experience
Experience-Based Technology Trust (Factors)
Experience-Based Trust Proxy (Attributes)
- Lazy User Theory

Figure 5. **Conceptual Framework for Methodology Leading to Technology Trust**

Experiment Methodology

This experiment investigates the formation of trust in technology and how it influences the adoption of autonomous systems for use in high-risk military applications. The formation of trust in technology is governed by two constructs: reason-based trust and experience-based trust. Existing literature presents the case for increased accuracy in technology selection through the development of experience-based trust. However, the development of experience-based trust is financially burdensome and takes much longer to form. In most military scenarios, developing experience-based trust presents high levels of risk for physical injury and harm.

Introduction

This experiment is designed to identify trust metrics and how they influence the formation of reason-based trust in autonomous systems used in high-risk military applications. The desired outcome of this work is the identification of attributes that can replace some of the burden required to develop experience-based trust. This research does not intend to demonstrate the validity of the theories behind technology acceptance; rather, this work investigates potential causal relationships between the manipulation of information and its effect on trust in technologies.

The experiment is conducted in two phases. Phase one is a group administered experimental survey that employs manipulations of multiple theories of technology acceptance in order to collect data on reason-based trust in autonomous systems. Phase two consists of administering the same survey following extensive field testing and experimentation of the phase one systems to provide external validity.

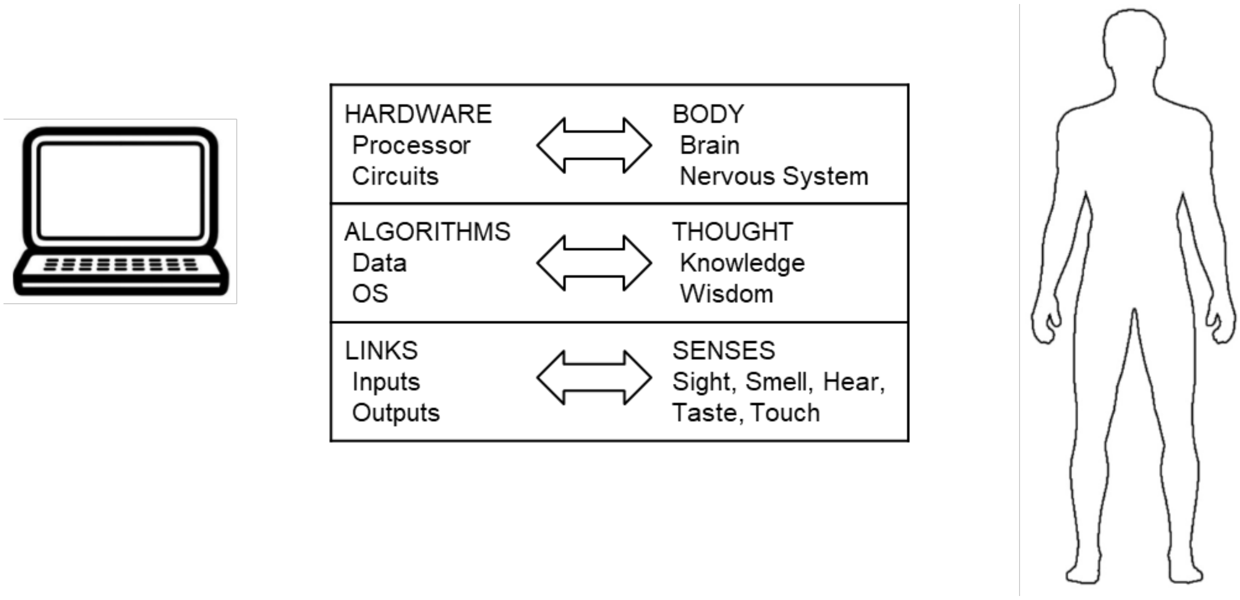
Metrics

The goal of this work is to study the influence of trust metrics on the acceptance of autonomous systems in high-risk applications. However, the complexity of modern technology makes it difficult to establish generalizable metrics that can function as a proxy for experience-based trust. One area of research relevant to establishing such metrics involves the use of anthropomorphism, the attribution of human traits to nonhuman entities, to increase a trustor's ability to accept and utilize technology. Waytz, Heafner, and Epley (2014) discuss the need for human-like mental models to consider technology as a trustworthy teammate. There are reported cases (Pak et al., 2012) where the tendency to anthropomorphize technology leads to situations in which humans give a higher degree of trust to a technology than is warranted. The inverse of this situation also exists in the development of a lack of trust in a human teammate caused by the introduction of technology with more capability and reliability. The work conducted by Waytz et al. (2014) includes a study that found test subjects were quicker to forgive a trustee's mistakes and stay calm in high-stress situations when the trustee was a technology with human-like attributes. This work provides a foundation for the establishment of our technology trust metrics.

HAL Score

In this work, we hypothesize that statistically significant differences will result in technology trust by anthropomorphizing an experience-based proxy. This hypothesis is based on leading theory used to increase cognition in students enrolled in a college-level computer architecture course. Over a period of 10 years, the author of this paper provided instruction to university year-three engineering students on the topics of digital design and computer architecture. The predominant challenge reported by students in end-of-year course evaluations was difficulty synthesizing the highly complex components of a computer into a usable system. Based on student feedback, a method for reducing complexity was developed by anthropomorphizing the components of a computer. This theory provided students with the context needed to understand how the pieces of a computer function together to create a whole system. The work resulted in increased student comprehension and an ability to describe a computer from the elemental circuits up to the most advanced concepts of computer engineering such as compilers and operating systems.

To develop the measurement system needed for an experience-based technology trust proxy, we introduce the anthropomorphic technology categories of *hardware*, *algorithms*, and *links* (HAL) as illustrated in Figure 6.



HARDWARE Processor Circuits	⇔	BODY Brain Nervous System
ALGORITHMS Data OS	⇔	THOUGHT Knowledge Wisdom
LINKS Inputs Outputs	⇔	SENSES Sight, Smell, Hear, Taste, Touch

Figure 6. **Anthropomorphic Technology Trust Metrics**

In order to increase the familiarity for military end-users, the metrics are established through the HAL scoring system. The values of each HAL subsystem initially range from 0 to 100 and lead to an equally weighted maximum score of 300. This scoring system is identical to the Physical Fitness Test (PFT) employed by the U.S. Marine Corps. The PFT scores three physical fitness tests, each scored from 0 to 100. The individual tests are pull-ups, crunches, and a three-mile run which result in a maximum combined score of 300. Future research intends to identify weights for the HAL score that accurately reflect the overall impact on trust. For the purposes of this experiment, we integrate the HAL score as a proxy for experience-based trust as shown in Figure 7.

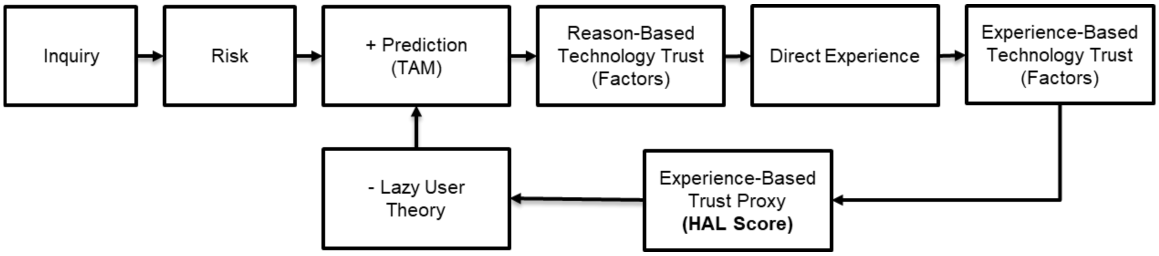

Inquiry
Risk
+ Prediction (TAM)
Reason-Based Technology Trust (Factors)
Direct Experience
Experience-Based Technology Trust (Factors)
- Lazy User Theory
Experience-Based Trust Proxy (HAL Score)

Figure 7. **HAL Score Experimental Model**

Data Analysis Plan

This study will employ Repeated Measures ANOVA. The variables in this study create a mixed design scenario. The first manipulated variable "metric" is a between-subjects factor and applies a treatment between two groups. The second manipulated variable "System Control" is a within-subjects factor, and each subject receives all three treatments of low (autonomous), medium (remote-control), and high (tethered control).

There are validity concerns due to fixed-effects seen in a repeated measure study. The participants may weight the variable "system control" based solely on whether or not they like the accompanying technology. To correct for such effects, techniques such as multilevel modelling may be employed in place of repeated measures analysis.

Success in this research is realized through statistically significant results leading to a new theory on the causal relationship between anthropomorphic trust metrics and the intent to use an autonomous system.

Table 3. Proposed Schedule

Date	**Process**
March–April 2019	Data Collection
April–May 2019	Data Analysis
May 2019	Initial Findings
July–August 2019	Field Testing
September 2019	External Validity Data Analysis
October 2019	Final Report

Conclusion

The topic of trust in technology is increasingly important to the DoD as outlined in the *Defense Science Board Study on Autonomy* (David & Nielsen, 2016), which states, "There is a need to build trust in autonomous systems while also improving the trustworthiness of autonomous capabilities. These are enablers that align RDT&E processes to more rapidly deliver autonomous capabilities to DoD missions."

This work involves the introduction of novel ideas to existing theories that relate to the formation of trust. This research focuses on the impact of trust towards the adoption of autonomous systems. We have established that trust involves a user assuming some level of risk. The only literature available on technology trust involves situations that expose users to insignificant levels of risk. We posit that our research conducted on technology used in high-risk military application will reveal causality not identified in previous trust research.

References

Adams, B. D., & Webb, R. D. (2002). Trust in small military teams. In *Proceedings of the 7th International Command and Control Technology Symposium* (pp. 1–20).

Boon, S. D., Holmes, J. G., Hinde, R. A., & Groebel, J. (1991). *Cooperation and prosocial behavior*. Cambridge, England: Cambridge University Press.

Castelfranchi, C., & Falcone, R. (2010). *Trust theory: A socio-cognitive and computational model*. John Wiley & Sons.

Cho, J.-H., Chan, K., & Adali, S. (2015). A survey on trust modeling. *ACM Computing Surveys (CSUR)*, *48*(2), 28.

David, R. A., & Nielsen, P. (2016). *Defense science board summer study on autonomy*. Washington, DC: Defense Science Board.

Devitt, S. K. (2018). Trustworthiness of autonomous systems. In *Foundations of Trusted Autonomy* (pp. 161–184). Springer.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, *27*(1), 51–90.

Hoff, K. A., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human Factors*, *57*(3), 407–434.

Kramer, R. M., & Tyler, T. R. (1996). *Trust in organizations: Frontiers of theory and research*. Thousand Oaks, CA: SAGE.

Lankton, N. K., McKnight, D. H., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems*, *16*(10), 880.

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS)*, *2*(2), 12.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334–359.

Pak, R., Fink, N., Price, M., Bass, B., & Sturre, L. (2012). Decision support aids with anthropomorphic characteristics influence trust and performance in younger and older adults. *Ergonomics*, *55*(9), 1059–1072.

Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in close relationships. *Journal of Personality and Social Psychology*, *49*(1), 95.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404.

Schaefer, K. E. (2016). A meta-analysis of factors influencing the development of trust in automation: Implications for understanding autonomy in future systems. *Human Factors*, 24.

Tétard, F., & Collan, M. (2009). Lazy user theory: A dynamic model to understand user selection of products and services. In *Proceedings of the 42nd Hawaii International Conference on System Sciences (HICSS '09*) (pp. 1–9). IEEE.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273–315.

Waytz, A., Heafner, J., & Epley, N. (2014). The mind in the machine: Anthropomorphism increases trust in an autonomous vehicle. *Journal of Experimental Social Psychology*, *52*, 113–117.

When Does It Make Sense to Acquire a Single Weapon System Design That Can Be Used in Both Manned and Unmanned Operational Modes?

Prashant R. Patel—is a Research Staff Member at the Institute for Defense Analyses (IDA) in the Cost Analysis and Research Division. His PhD is in aerospace engineering and his master's degree is in space systems, both from the University of Michigan. Some of his past projects at IDA include industrial base studies, developing models to visualize the cost-performance trade space of weapon systems, adaptability of weapon systems, and short-of-war actions by U.S. adversaries. [ppatel@ida.org]

David M. Tate—joined the research staff of the Institute for Defense Analyses' (IDA) Cost Analysis and Research Division in 2000. Prior to that, he was an Assistant Professor of Industrial Engineering at the University of Pittsburgh, and the Senior Operations Research Analyst (Telecom) for Decision-Science Applications, Inc. At IDA, he has worked on a wide variety of resource analysis and quantitative modeling projects related to national security. These include an independent cost estimate of Future Combat Systems development costs, investigation of apparent inequities in Veterans' Disability Benefit adjudications, and modeling and optimization of resource-constrained acquisition portfolios. Tate holds bachelor's degrees in philosophy and mathematical sciences from the Johns Hopkins University, and MS and PhD degrees in operations research from Cornell University. [dtate@ida.org]

Abstract

There is a strong push to change from manned toward both unmanned and optionally manned systems within the Department of Defense. There are significant open questions about how the manned versus unmanned versus optionally manned options influence costs, adaptability, operational utility, and suitability for missions. The Institute for Defense Analyses developed an approach to address these questions that links underlying physical attributes and engineering relationships to mission attributes and costs. We discuss this approach, where it fits into the acquisition process, and how it can be used to quantitatively inform the unmanned versus optionally manned discussions at both a system level and fleet level.

Background

Today's operational environment is complicated by many requirements that compete against one another for design resources (Freedberg, 2019).[1] Of course, this is not the primary challenge—after all, trade studies have been around for a long time. The primary challenge is characterizing the trades among system attributes (including cost) in a manner that can inform and guide leadership decisions prior to the Analysis of Alternatives (AoA) stage, rather than simply defending the selected alternative after the fact. In the end, this requires methods that leaders understand and visualizations that they can use. These

[1] "We were under three entirely different organizations previously," Maj. Gen. Cedric Wins said. So RDECOM scientists and engineers would often be eager to offer their expertise to the future concepts teams, but "sometimes, though, quite frankly we might be late to the game," he said. The futurists might have committed to a particular technology without realizing there was a better alternative or, worse yet, without realizing it just wasn't ready for the real world.

methods must expose the implications of choices rather than mask them, long before detailed designs for the alternative approaches exist.

The Institute for Defense Analyses' (IDA's) trade space framework—Deducing Economically Realistic Implications Via Engineering (DERIVE)—links engineering and physics analysis, operational constraints, and semi-parametric cost estimates. The goal is to increase the efficiency of the acquisition process by reducing friction between the program office, the Services, the Joint Staff, and the Office of the Secretary of Defense (OSD), especially at program initiation and during the early stages of development.

IDA designed the DERIVE framework to link important technical inputs to programmatic and operational outputs in a straightforward, traceable, and transparent manner. The framework provides an analytic structure that could be used to build understanding and communicate intent. It could be especially helpful for programs whose complex interactions between requirements, operational restrictions, and technology—rather than any individual issue—drive acquisition outcomes.

Trade Space

The use of trade studies in engineering is not new. It has a long history in the technical community and has now been formally adopted into the Department of Defense (DoD) acquisition decision-making process. Recent experiences suggest that the Services' trade-space tools are being used to inform their internal deliberations. However, several recent new-start proposals have been the subject of follow-on trade studies and amended AoA efforts, suggesting room for improvement. In particular, past trade studies have generally not been able to address high-level trades between competing design families (e.g., conventional helicopters vs. tilt-rotors), or affordability implications of design choices.

Schedule delays associated with follow-on analyses can be avoided if the trade study processes and analytical outputs are structured to support both user and oversight objectives. The outputs of IDA's DERIVE framework are constructed to achieve this goal by enhancing traceability and transparency of inputs, outputs, and decision-making.

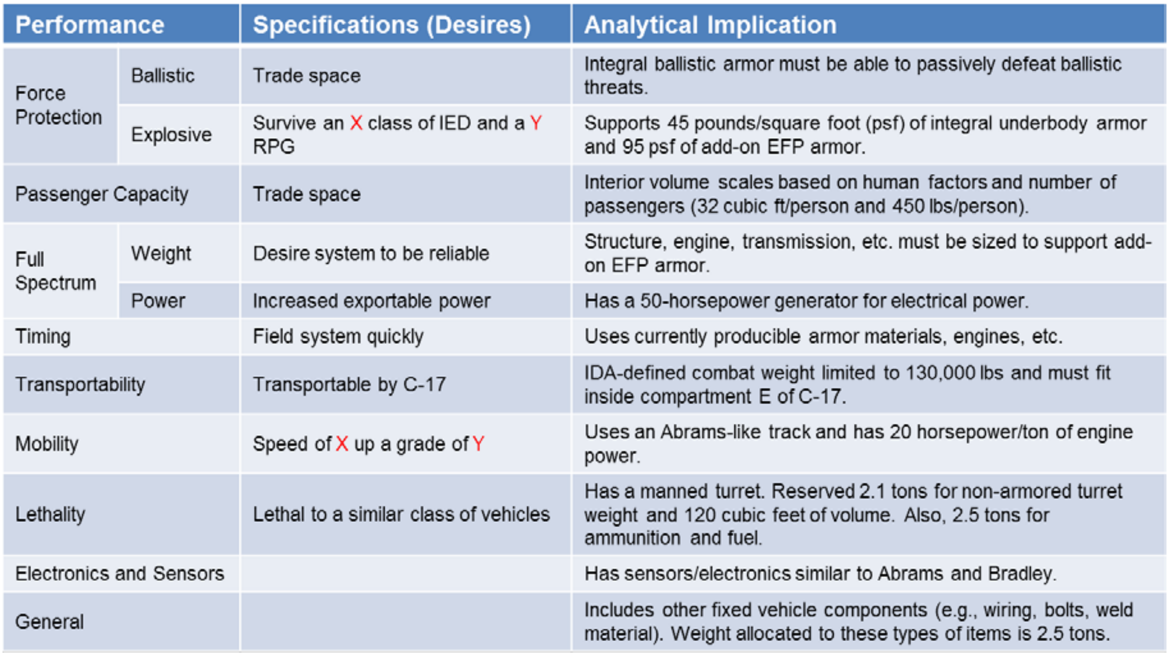
Traceability

Traceability is used by systems engineers to manage technically complex endeavors by flowing down program objectives into discrete technical goals. Alternatively, students employ traceability to demonstrate to professors that they have a firm grasp of the nature of problems even if small errors are present in the analysis. Traceability can also be leveraged by the Services and program offices to demonstrate that they have rigorously analyzed the operational environment and have a firm understanding of the technical issues and programmatic consequences of a new program.

The DoD asked IDA to develop and demonstrate DERIVE on a generic infantry fighting vehicle (IFV). The results of that effort will be used below to illustrate how DERIVE's outputs are designed to foster traceability.

Creating traceability requires exposing the objectives of the program, how they relate to technical assumptions, and how the various elements interact to drive results. An output of the DERIVE process traces the desired capabilities to the commensurate technical inputs. shows how key performance and programmatic attributes can be mapped to specific technical requirements for an IFV.

Table 1. Performance and Technical Traceability Matrix

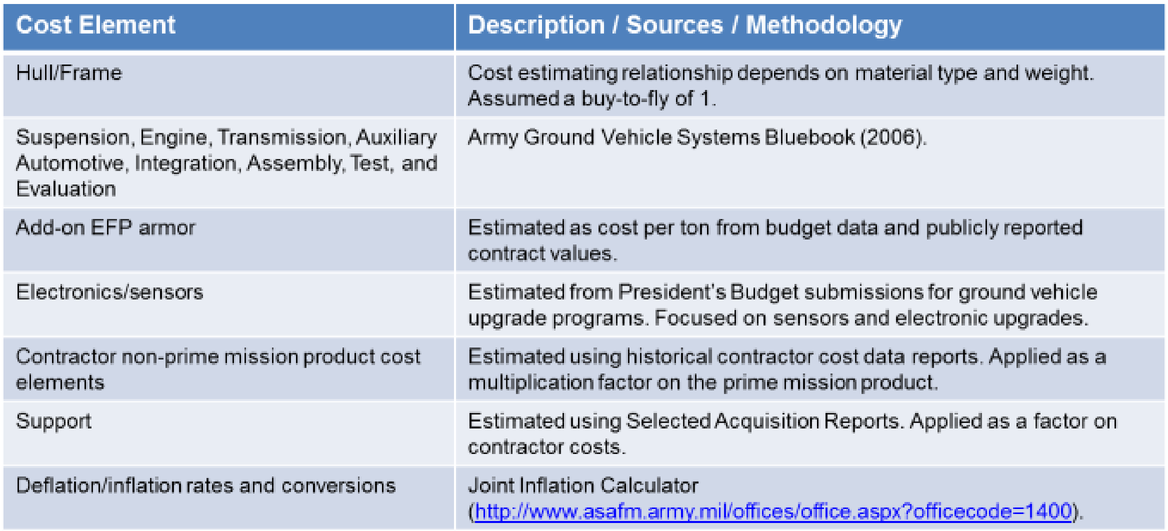


Performance		Specifications (Desires)	Analytical Implication
Force Protection	Ballistic	Trade space	Integral ballistic armor must be able to passively defeat ballistic threats.
	Explosive	Survive an X class of IED and a Y RPG	Supports 45 pounds/square foot (psf) of integral underbody armor and 95 psf of add-on EFP armor.
Passenger Capacity		Trade space	Interior volume scales based on human factors and number of passengers (32 cubic ft/person and 450 lbs/person).
Full Spectrum	Weight	Desire system to be reliable	Structure, engine, transmission, etc. must be sized to support add-on EFP armor.
	Power	Increased exportable power	Has a 50-horsepower generator for electrical power.
Timing		Field system quickly	Uses currently producible armor materials, engines, etc.
Transportability		Transportable by C-17	IDA-defined combat weight limited to 130,000 lbs and must fit inside compartment E of C-17.
Mobility		Speed of X up a grade of Y	Uses an Abrams-like track and has 20 horsepower/ton of engine power.
Lethality		Lethal to a similar class of vehicles	Has a manned turret. Reserved 2.1 tons for non-armored turret weight and 120 cubic feet of volume. Also, 2.5 tons for ammunition and fuel.
Electronics and Sensors			Has sensors/electronics similar to Abrams and Bradley.
General			Includes other fixed vehicle components (e.g., wiring, bolts, weld material). Weight allocated to these types of items is 2.5 tons.

Cross-referencing the technical assumptions and desired capabilities in a single, compact form provides two benefits. First, it allows the program developers to articulate clearly the user's goals and the technical requirements necessary to achieve those goals. Second, it allows the oversight community to understand the potential loss of capability if there are technical shortfalls during development.

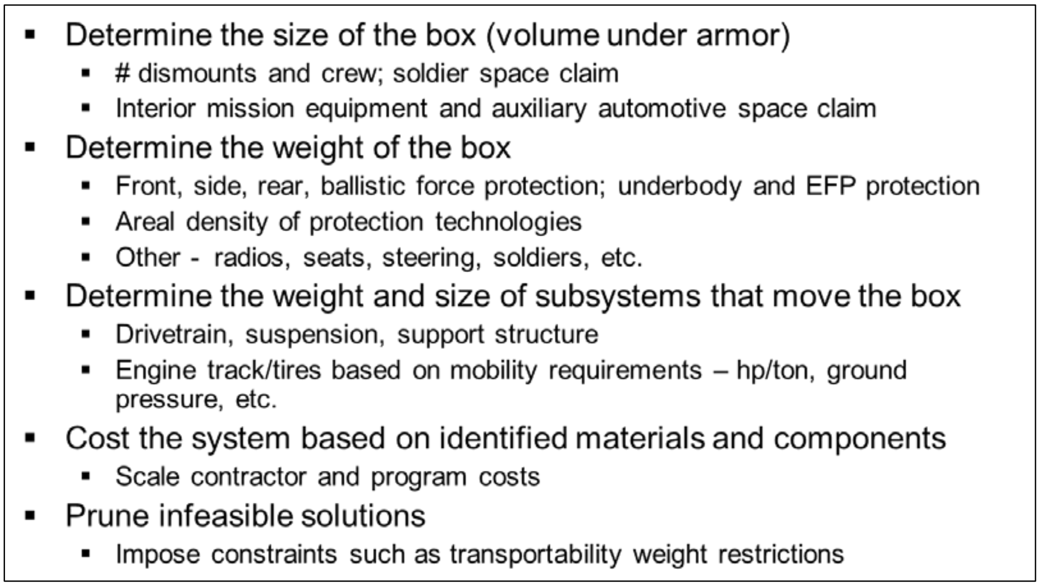
Similarly, shows how cost traceability can be achieved. Various cost categories are mapped to the data sources and assumptions used in generating the cost estimate. This traceability matrix allows oversight organizations to qualitatively assess the riskiness and fidelity of the estimate.

Table 2. Cost Elements and Costing Assumptions and Data Sources



Cost Element	Description / Sources / Methodology
Hull/Frame	Cost estimating relationship depends on material type and weight. Assumed a buy-to-fly of 1.
Suspension, Engine, Transmission, Auxiliary Automotive, Integration, Assembly, Test, and Evaluation	Army Ground Vehicle Systems Bluebook (2006).
Add-on EFP armor	Estimated as cost per ton from budget data and publicly reported contract values.
Electronics/sensors	Estimated from President's Budget submissions for ground vehicle upgrade programs. Focused on sensors and electronic upgrades.
Contractor non-prime mission product cost elements	Estimated using historical contractor cost data reports. Applied as a multiplication factor on the prime mission product.
Support	Estimated using Selected Acquisition Reports. Applied as a factor on contractor costs.
Deflation/inflation rates and conversions	Joint Inflation Calculator (http://www.asafm.army.mil/offices/office.aspx?officecode=1400).

Finally, the logic used to estimate the costs and performance of the IFV trade space is described in Figure 1. In sum, the DERIVE framework helps program developers and the acquisition oversight community build a common understanding of the key technical, operational, and cost drivers of new capabilities being sought by the department.



- Determine the size of the box (volume under armor)
  - # dismounts and crew; soldier space claim
  - Interior mission equipment and auxiliary automotive space claim
- Determine the weight of the box
  - Front, side, rear, ballistic force protection; underbody and EFP protection
  - Areal density of protection technologies
  - Other - radios, seats, steering, soldiers, etc.
- Determine the weight and size of subsystems that move the box
  - Drivetrain, suspension, support structure
  - Engine track/tires based on mobility requirements – hp/ton, ground pressure, etc.
- Cost the system based on identified materials and components
  - Scale contractor and program costs
- Prune infeasible solutions
  - Impose constraints such as transportability weight restrictions

Figure 1. **Outline of Process Used in Creating Infantry Fighting Vehicle Trade Space**

Transparency

The DERIVE framework improves the transparency of the analyses supporting acquisition decisions. Figure 2 shows an output of the DERIVE framework for the IFV example. It enhances transparency by illustrating the entire trade space rather than a few point designs. Showcasing the full trade space demonstrates the thoroughness of the investigation and reduces the possibility of having to include additional cases. Also, instead of using a value function, the analysis simply highlights the desired point solutions and lists the rationale for the decision and the relevant trade-offs that were considered and accepted as part of the decision-making process. Showing trade space data, the rationale, and the resulting decision together serves to enhance trust, convey thoroughness, and reduce institutional friction.

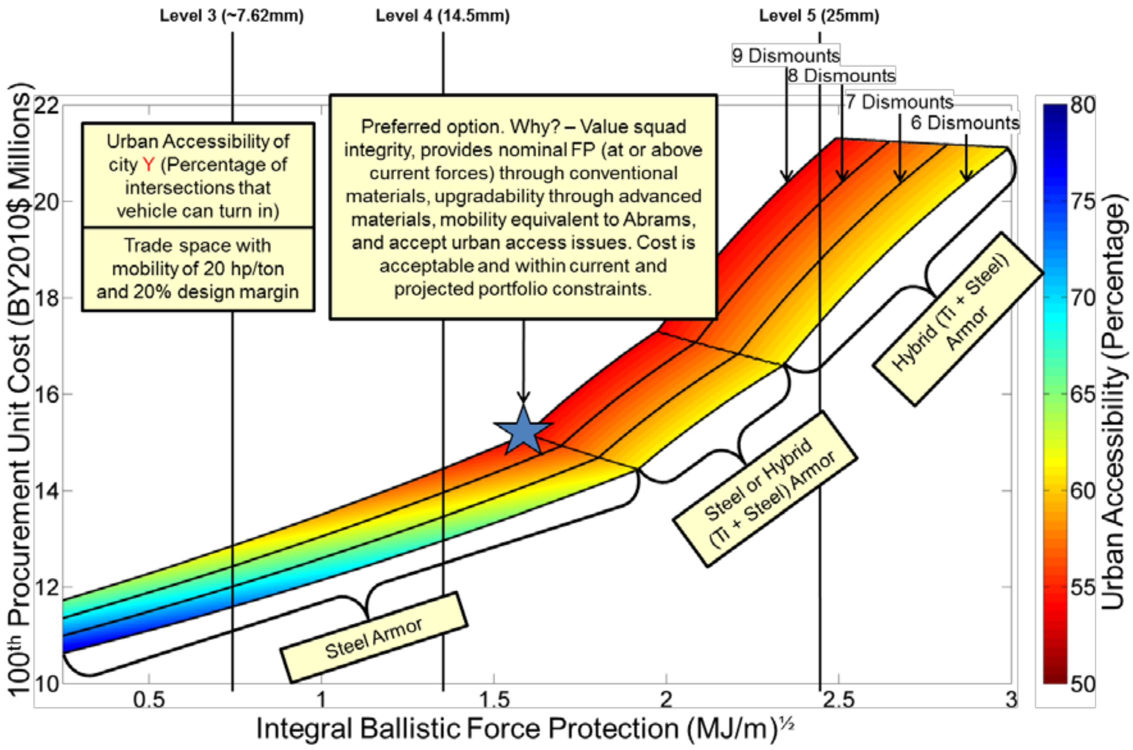


Figure 2. **Infantry Fighting Vehicle Trade Space with Logic for Decision**

The outputs from DERIVE also make certain difficult trades obvious. For example, it is clear from Figure 34 that no vehicle carrying six or more dismounts can provide both full urban trafficability and force protection level 3 or higher. If there is a mission need for well-protected fighting vehicles in urban environments, they will need to carry fewer personnel per vehicle. Similarly, force protection level 5 can only be obtained using advanced armors, with corresponding unit cost consequences.

Thought Experiment 1: Urban Counterinsurgency

Given mission need for a fighting vehicle that can maneuver in 90% of urban terrain and provide force protection level 3 or higher, what are the available options? Figure 2 shows that such a vehicle cannot carry very many people; the space claim of human passengers induces a positive feedback on required cubic feet, and thus on areal surface to be armored, and thus on weight. This has consequences for concepts of operations—if it is not possible to preserve squad integrity in urban environments while preserving force protection levels, either squads will need to be divided or force protection levels will need to be reduced. Either of these leads to changes in how the force will fight. They key is that exposing these issues early puts the warfighter in charge of making the decision of what they value, since they ultimately have to manage the consequences.

Thought Experiment 2: Optionally Manned Vehicles

Recent advances in remotely piloted vehicle technologies and artificial intelligence (AI)–enabled autonomy have increased interest in optionally manned vehicles—that is, vehicles that are typically operated as manned vehicles with a human driver, but can sometimes be operated as remotely piloted or even autonomous vehicles. What are the costs and benefits of optional manning? Under what circumstances would an optionally manned design be preferable to an unmanned design, or to a mixed fleet of manned and unmanned designs? We can use DERIVE to investigate these questions.

In general, the principal benefits of unmanned systems arise from the absence of those requirements related to the presence of human passengers. Human beings and their equipment are heavy; they occupy space; they require environmental conditioning and protection against threats. Unmanned systems can thus avoid the weight associated with humans, their equipment, additional armor, heating and air conditioning systems, air purification systems, doors, seats, visual displays, manual controls, and so forth. They can be smaller than manned systems, potentially able to operate in more confined spaces and with lower observability.

Optionally manned systems do not share these benefits. Instead, they incur all of the weight and space penalties of manned vehicles, plus additional requirements to support remote operation. This might include additional sensors, communications links, and onboard computational power. These added systems must also be configured so as not to interfere with manned operations—so that, for example, any cameras that provide the "driver's view" for remote operation must not interfere with the driver's sight lines during manned operations.

In the end, the business case for an optionally manned platform must rest on the mix of missions the system is envisioned for, and the concept of operations that would make a mixed fleet of manned and unmanned systems impractical. DERIVE could be used to quantify these trades, informing decision-makers about the operational and cost consequences of design choices and force mixes before committing significant resources.

Conclusion

DERIVE and similar approaches provide a framework that can be used to engage and improve acquisition outcomes. DERIVE fuses a variety of information sources (capabilities, operational, technical, and cost) to enable more thorough analyses in support of decision-making and to reduce friction between program developers and the acquisition oversight community. DERIVE can also serve to make fundamental trades more apparent to senior decision-makers, avoiding misunderstandings about what is feasible and focusing the discussion on the relevant warfighter values.

References

Freedberg, S. J., Jr. (2019). Army R&D chief: "I don't think we went far enough"—But Futures Command can. *Breaking Defense*. Retrieved from https://breakingdefense.com/2019/02/army-rd-chief-i-dont-think-we-went-far-enough-but-futures-command-can/

Gillingham, D. R., & Patel, P. R. (2013). *Method of estimating the principal characteristics of an infantry fighting vehicle from basic performance requirements* (IDA Paper P-5032). Alexandria, VA: Institute for Defense Analyses.

Acknowledgments

The authors thank David Gillingham for building the sub-system models and showcasing the value of this approach on the JLTV program, David Sparrow for his tireless support of this effort and attempts to improve early acquisition outcomes, Brian Gladstone for his assistance in enabling us to generate this talk and pushing us to do it, and Paul Mann for hosting and leading the discussion session.

Panel 10. DoD Contract Management Perspectives

Wednesday, May 8, 2019	
2:15 p.m. – 3:30 p.m.	**Chair: Dr. Rene Rendon,** Associate Professor of Acquisition Management, Naval Postgraduate School ***Exploring the Effect of Waivers to the Non-Manufacturing Rule on Contract Awards to Small Businesses*** William Muir, Naval Postgraduate School; Timothy Hawkins, Western Kentucky University; and Michael Gravier, Bryant University ***Commercial Aircraft Pricing: Models, Applications, and Lessons Learned*** Bruce Harmon, Institute for Defense Analyses ***Towards the Dynamic Contracting of Verification Activities With Set-Based Design: An Initial Model of Rework*** Alejandro Salado and Peng Xu, Virginia Tech

Dr. Rene Rendon—is a nationally recognized authority in the areas of supply management, contract management, and project management. Dr. Rendon is currently on the faculty of the United States Naval Postgraduate School, where he teaches in the MBA and Master of Science programs. Prior to his appointment at the Naval Postgraduate School, he served for more than 22 years as an acquisition and contracting officer in the United States Air Force, retiring at the rank of lieutenant colonel. His Air Force career included assignments as a warranted contracting officer for the Peacekeeper ICBM, Maverick Missile, C-20 (Gulfstream IV), and the F-22 Raptor. [rgrendon@nps.edu]

Exploring the Effect of Waivers to the Non-Manufacturing Rule on Contract Awards to Small Businesses

William A. Muir—PhD, is an Assistant Professor at the Naval Postgraduate School, Graduate School of Business and Public Policy. His research focuses on public-sector supply management, productivity and efficiency of logistics organizations, and inventory dynamics. His research has appeared in the *Journal of Business Logistics*, *Journal of Purchasing and Supply Management,* and the *Journal of Public Procurement*. [wamuir1@nps.edu]

Michael J. Gravier—PhD, CTL, is Associate Professor of Marketing and Global Supply Chain Management at Bryant University. Dr. Gravier has published articles on the factors affecting supply chain strategies and relationships such as transportation, ethics, procurement practices, and technological obsolescence. He has also published and presented on logistics and supply chain pedagogy. His research has appeared in *International Journal of Logistics Management*, *Journal of Purchasing and Supply Management*, *Supply Chain Management: An International Journal*, *Journal of High Technology Management Research*, *Journal of Public Procurement*, and *Journal of Business Ethics.* [mgravier@bryant.edu]

Timothy G. Hawkins, Lt Col (Ret.), USAF—PhD, CPCM, CPM, is an Associate Professor in the Department of Marketing at Western Kentucky University. His current research interests include performance-based logistics, electronic reverse auctions, procurement ethics, buyer-supplier relationships, strategic sourcing, services procurement, and supplier performance management. Prior to his academic career, Dr. Hawkins worked in Global Procurement for NCR Corporation and served as a warranted contracting officer for the U.S. Air Force. Dr. Hawkins has published articles on procurement and logistics topics in scholarly publications such as the *Journal of Business Logistics*, *Journal of Supply Chain Management*, *Journal of Business Research*, *Journal of Purchasing and Supply Management*, *International Journal of Logistics Management*, *Industrial Marketing Management*, *Journal of Business Ethics*, *Supply Chain Management: An International Journal*, and the *Journal of Public Procurement*. [timothy.hawkins@wku.edu]

Abstract

The U.S. government regularly participates as a buyer in industrial markets where products are customarily sold through indirect marketing and distribution chains, separating buyers from manufacturers. In many cases, these marketing, distribution, and store-front activities add significant value for buyers, such as through pre- and post-sale service and support, improvements to product availability, and reductions in per-unit pricing (e.g., via economies due to warehousing, transportation, and ordering processes). Accordingly, the government (U.S. Small Business Administration) has, in some instances, issued class waivers to the requirements of the “non-manufacturer rule” (15 U.S.C. § 657s) when no small business manufacturers exist for a product, such that contracts can be set aside for competition among small business non-manufacturers. This study models the effectiveness of class non-manufacturer rule waivers on the utilization of small business concerns. The purpose of the research is to obtain a better understanding of market and industry conditions in which these waivers are successful at driving small business utilization, as well as conditions where class waivers, once issued, tend to be poorly utilized. A time series panel of data derived from several archival sources was used to estimate a fractional response model with a Bernoulli quasi-maximum likelihood estimation methodology. Findings indicate that NMR waivers work best to increase small business utilization in industries characterized by low concentration and low levels of price inflation. Understanding these factors will inform policy and regulation.

Introduction

The Small Business Act of 1953 requires that a *fair proportion* of contract dollars be awarded, or set aside, to small businesses (Sakallaris, 2007). This is not a trivial directive as the public sector constitutes a huge market, approximately $2.1 trillion annually in the United States alone. This means that a tremendous amount of those public funds—$90.7 billion in fiscal year 2015 (Federal Procurement Data System, 2015)—is deliberately funneled to small businesses at all levels (municipal, county, state, and federal) as a matter of public policy aimed at achieving socio-economic benefits. The current, government-wide procurement goal stipulates that at least 23% of all federal government contracting dollars should be set aside for small businesses with targeted set-asides for Women Owned Small Business (5%), Small Disadvantaged Business (5%), Service Disabled Veteran Owned Small Business (3%), and Historically Underutilized Business Zones (3%).

Not only are socio-economic procurement programs important to the public sector (Denes, 1997), they are also critical to the private sector. Small businesses constitute approximately half of the private-sector economy and 99% of all businesses (U.S. Small Business Administration [SBA], 2012). They account for 90% of exports and innovations (Cullen, 2012). Small- and medium-sized enterprises (SMEs) are important to economic growth (Thurik & Wennekers, 2004; Wennekers & Thurik, 1999). SMEs differ from large businesses in job creation, strategic flexibility, and innovation (Audretsch, 2007). Consequently, economies with more SMEs are more competitive and have higher growth rates than those with fewer SMEs (Audretsch et al., 2006).

Small- and medium-sized businesses are a fundamental element of the health and economic viability of the United States (Sperling & Mills, 2012). According to the National Economic Council, over the past 20 years, small and new businesses in the United States have been responsible for creating two out of every three net new jobs and employ half of the private sector workforce (Sperling & Mills, 2012). More specifically, small businesses are a foundational element to communities (i.e., populations less than 10,000 people) and play a significant role in the economic health of those communities (Yoshida & Deyle, 2005). Small businesses also service as critical participants in the supply chain (Qi et al., 2014; Logozar, 2013).

Unfortunately, while the U.S. federal government annually seeks to award 23% of contract dollars to small businesses, it often fails to fully achieve its small business goals (FPDS, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015). Impediments to small business contracting include contract bundling, strategic sourcing resulting in supplier rationalization, a lack of accountability for achieving socio-economic goals, a lack of small businesses in some industries, and many small businesses' lack of interest in performing government work (Grammich et al., 2011).

Given the criticality of small businesses to long-term economic viability, several laws, regulations, and programs have been promulgated to advance their cause. One such rule is the non-manufacturer rule (NMR), enacted by Section 303(h) of Public Law

100-656 and Section 210 of Public Law 101-574. According to 13 C.F.R. § 121.406,[1] for a firm to qualify and represent itself as a small business concern on a federal procurement for an end item, it must either be the manufacturer (or producer) of that end item or meet additional criteria to qualify as a small non-manufacturer, including supplying the end item of a small business manufacturer, processor, or producer. As of 2016, this rule applies exclusively to acquisitions in excess of the simplified acquisition threshold, although smaller acquisitions were previously subject to the rule (81 FR 34243). Thus, the NMR allows a small business dealer who does not manufacture an end item (e.g., a wholesaler, a distributor) to compete as a small concern under set-aside federal contracts to supply that product, provided that the manufacturer is a small business located in the United States and that certain other requirements of the NMR are satisfied (FAR 19.001). However, in some industries, or for some end items or classes of end items, no small business manufacturers exist. In such cases, a waiver to the NMR could be requested—in the case of a class waiver, by the prospective small business supplier, by the contracting officer, by an industry group, or by some other entity—from the Small Business Administration (SBA) such that, for example, a small business distributor can supply a product manufactured by a large business and still qualify as a small business concern under a set-aside contract.

Granting class waivers in such markets dominated by large businesses should, in theory, open opportunity for small businesses distributors to secure federal contracts. From the buyer’s perspective, opening up markets to small business distributors should expand the available supply base under a small business set-aside, further enhancing competition and, in turn, reducing purchase prices (Chiang, Chhajed, & Hess, 2003). Furthermore, making more small businesses eligible to provide certain products means that more requirements can be set aside for small businesses, thereby increasing the amount of dollars awarded to small businesses and helping buying agencies meet their socio-economic goals.

To date, however, the contribution of class waivers to the NMR to small businesses’ success in winning contracts is unknown. The purpose of this research, therefore, is to explore whether industry characteristics influence the effectiveness of class NMR waivers with regard to achieving their intended goal of improving small business utilization on federal purchases, and if so, to what degree. This research is important due to its implications not only for socio-economic program design but also for effective and efficient channel design. Allowing small businesses to compete as intermediaries broadens the competitive base of federal buying agencies; thus, economic efficiencies are also at stake.

Generally, research has ignored key micro-level factors, especially in the context of small businesses. There are roughly 28 million small businesses in the United States, yet they are often ignored, despite the fact that ignoring SMEs in research is “in fact totally inappropriate” (Spence & Lozano, 2000, p. 43). Our scan of the last 10 years of the *Journal of Small Business Management*, *Journal of Small Business Strategy*, and *Journal of Small Business and Entrepreneurship* revealed only 48 B2B articles

[1] See, for instance, the requirements contained within Federal Acquisition Regulation (FAR) 52.219-1, *Small Business Program Representations*, which state that a firm representing itself as a small business concern must satisfy the criteria in 13 C.F.R. § 121.406.

representing 8% of all contributions. Most of these articles address various aspects of franchising. Furthermore, research in a business-to-government context is almost non-existent. Only one article (Albano et al., 2015) addressed any aspect of small businesses in the public sector.

The remainder of this work is organized as follows. Underlying theory relevant to waivers to the NMR is synopsized. Next, the study presents the research design and methodology, and then the study provides an analysis of the proposed model and reports the findings. Lastly, the study offers a summary discussion, including conclusions and implications.

Literature Review

Of all of the elements of a value chain, the marketing channel ranks highly in importance (Krafft, Goetz, Mantrala, Sotgiu, & Tillmanns, 2015), with wholesale distribution comprising revenues of $5.2 trillion in 2017. Nevertheless, they are not fully understood. Scholars have called for a more unifying theory of distribution channels (Ingene & Parry, 1995). Similarly, omni-channel research is largely void of theoretical grounding (Erdem, Kotzab, Teller, Yumurtaci Hüseyinoglu Isik, & Pöppelbuß, 2018). The interface between industry and government has also been identified as a promising research avenue (Krafft et al., 2015).

Socio-economic programs have been used by both government and private sectors to develop local economies, develop labor capabilities, and expand their customer base. This macro strategy is well founded as “states with higher proportions of very small business employment do indeed experience higher levels of productivity growth, and Gross State Product growth, while having less wage inflation and lower unemployment rates” (Robbins et al., 2000, p. 293). Sourcing from small, minority-owned enterprises can increase job creation and economic development in distressed regions (Carter et al., 1999; Walker & Preuss, 2008). In turn, the income from these businesses and employees thereof expand the firm’s customer base (Ram & Smallbone, 2003).

NMR waivers are one tool that allows government to fence off large business manufacturers and distributors from competing against small business distributors for contracts from the federal government segment. The lack of research into the contribution of class NMR waivers or the circumstances conducive to their effectiveness creates a sub-optimal situation where NMR waiver success—and the factors influencing or impeding success—are not well understood. Evidence suggests that industry characteristics significantly determine the success or failure of selected channels. NMR waivers provide remedy for small businesses who must deal with power and conflict against large businesses.

Research on channel power and conflict emerged as a distinct research group in the 1990s by a study of the intellectual structure of retailing research (Chabowski, Hult, & Mena, 2011). At this time, channel competition was also identified as a distinct group of research. Matters of channel design continue to intrigue marketing scholars. Relevant to NMR waivers, a content analysis of recent channels research (2010–2012) identified *vertical competition* among seven key categories (Young & Merritt, 2013). Improving channel performance and coordination as well as lessening channel conflict and power were found to be prominent research themes, although with regard to small businesses, research has a strong franchise focus. The focus on the tension between small franchisees and large franchisors suggests that opportunistic use of power by larger channel members can have long-lasting effects on trust and performance (Winsor et al., 2012). This calls into question the efficacy of NMR waivers to reassure or encourage small businesses to engage in industries characterized by many large companies.

Another stream of research surrounding omni-channel retailing identified three areas: channel demand side, channel supply side, and channel management and strategy (Erdem et al., 2018). The channel supply side area focuses on supply chain processes, with one group of papers addressing multi-channel fulfillment strategies. This particular stream of research is underserved while considered a promising frontier of inquiry (Erdem et al., 2018). In general, it appears that direct channels can be profitable when channel members (manufacturers and retailers) share profits. This suggests that in an environment with high price pressures (highly inflationary), small businesses will be at a disadvantage with regard to negotiating profit sharing with large manufacturers.

From a supply management perspective (i.e., a buyer's), channel design presents a special case of strategy. With increased outsourcing, supply managers often play the role of integrator, stitching together capabilities of suppliers into seamless processes ranging from product development to delivery (Parker & Anderson, 2002). Research suggests that the integration of product development, manufacturing process design, and supply chain design can contribute to a competitive advantage (Ellram, Tate, & Carter, 2007). The competitive advantage results from parallel cross-functional coordination and strong supplier involvement, which suggests that industries characterized by many small businesses may achieve more success and benefit more from NMR waivers.

Firms concerned about corporate social responsibility often look to promote socio-economic goals. In this case, channels can be customized to the value offering as buyers seek qualified small business suppliers. Notwithstanding, best practices in supply management suggest that, in some circumstances, buyers should develop capabilities in strategic suppliers—termed *supplier development* in the literature (Krause, 1997). This, of course, alters the supply chain for certain material and component inputs.

A key question in marketing channels is, *Under what circumstances is a certain channel structure appropriate?* Class waivers to the non-manufacturer rule provide an interesting test-bed to examine not only the effectiveness of a federal policy, but also the conditions under which a direct channel will prevail over an indirect channel.

> H1: There will be a negative, two-way interaction between industry-level price inflation and issuance of class waivers to the non-manufacturer rule, such that a waiver's positive effect on small business utilization is attenuated when industry-level prices are highly inflationary.

> H2: There will be a negative, two-way interaction between industry concentration and issuance of class waivers to the non-manufacturer rule, such that a waiver's positive effect on small business utilization is attenuated when industries are highly concentrated.

> H3: There will be a positive, two-way interaction between the proportion of small firms in an industry and issuance of class waivers to the non-manufacturer rule, such that a waiver's positive effect on small business utilization is amplified when there is a high proportion of small firms in an industry.

Data and Measures

The SBA's class waiver list as of January 1, 2015, includes 139 waivers covering 72 NAICS categories (SBA, 2018), a majority of which cover chemicals, adhesives, metals, carpet, storage tanks, construction equipment, turbines, ammunition, office copiers, automobiles, computer equipment, televisions, medical equipment, aircraft, and furniture.

To test the research hypotheses, a time-series panel was constructed using multiple sources of archival data. Data on the issuance of class wavers to the non-manufacturing rule by the SBA were collected from the administration's current class waiver list (SBA, 2018). This list contains information for each class waiver, including the applicable industry as identified the by North American Industry Classification System (NAICS) code, the type of product and an effective date for the waiver (the date the class waiver was posted in the Federal Register). A total of 148 class waivers are on the list, with waivers issued for products manufactured across 77 industries. Example class waivers include ice-making machinery, turbines, hospital furniture, ammunition, and turboprop aircraft.

Data on the government's utilization of small suppliers were collected from the Federal Procurement Data System-Next Generation (FPDS-NG), which catalogs unclassified transactions between federal agencies and firms for the purchase of goods and services (Eckerd & Girth, 2017). In the context of government purchasing, a "small" firm is formally defined for each industry by the SBA. Criteria for determining firm size include the number of employees and/or average annual revenues. In FPDS-NG, government buyers report for each purchase whether the purchase was made to a small firm, based on representations made by the firm at the time of the purchase. We collect FPDS data on contracts across the U.S. government. Our period of analysis begins with Fiscal Year 2007, as significant improvements to FPDS data quality followed the passage of the Federal Funding Accountability and Transparency Act of 2006 (Lewis, 2017). We do not collect FPDS data for transactions after 2015, as certain industry establishment data (described below) are not available beyond 2015.

Lastly, to obtain information on industry characteristics, we obtain time-series observations on industries from the U.S. Bureau of Labor Statistics and the U.S. Census Bureau. These data are detailed in the following sections. All economic data were collected in their unseasonal form.

Dependent Variable

We measure federal performance on the utilization of small businesses concerns as the proportion of awards to small businesses within a given NAICS code, on a given annual measurement occasion, as reported in FPDS-NG. We refer to this variable as *UTILIZATION*. The federal government similarly uses proportions to measure small business utilization, as has prior research into the determinants of performance of small business contracting programs (Smith & Fernandez, 2010).

Treatments

Our primary explanatory variable, *TREATMENT*, reflects waiver issuance and is identified by an occurrence of one or more non-manufacturer waivers issued to an industry in succession (i.e., within a six-month period), between the years 2007 and 2015. For instance, three class waivers were issued in August 2010 to the computer storage device manufacturing industry (NAICS 334112) for automated data processing input/output and storage devices, support equipment and supplies, reflecting a treatment. A total of 20 treatments occurred during the period of analysis, to a total of 20 industries.

Moderators

Within H1, H2, and H3, we hypothesized that three industry-level moderators would moderate (amplify or attenuate) the effects of non-manufacturer rule waivers on small business utilization. The first moderator, *CONCENTRATION*, reflects the degree to which market share is concentrated within firms in an industry. Industry concentration data was obtained from the U.S. Census Bureau,[2] of which the most recent data available is from the 2012 economic census. *CONCENTRATION* is measured using the 50-firm Herfindahl-Hirschman Index (HHI), a summation of squared market shares. Higher HHI values reflect greater concentration and may range to a maximum value of 10,000. We utilize 2012 HHI observations as our *CONCENTRATION* measure, and log-transformed the values to account for skew. As the economic census is performed every five years, the only other possible index is from 2007, at the start of our analysis. [3] As we later explain, we reserve the 2007 index instead for propensity score matching of treated industries (those receiving waivers) with untreated industries. Thus, our measure of *CONCENTRATION* remains time-invariant over the period of analysis.

The second moderator, *SMALLPROP*, reflects the proportion of small firms in each industry, at each annual measurement occasion, operationalized as the proportion of firms in an industry having less than 500 employees.[4] Data on the distribution of firms within industries by firm size were obtained from the U.S. Census Bureau's Statistics of U.S. Businesses (SUSB),[5] which provides distributional data on enterprises in the U.S. economy by size and industry. SUSB provides data on both firms and establishments, where establishments are locations where work is performed (e.g., business locations) and where one or more establishment may be nested within a firm (Headd & Kirchhoff, 2009). We exclusively utilize firm data when calculating *SMALLPROP.*

The third moderator, *PRICEINDEX*, is an annual, aggregate measure of the prices received by domestic producers within an industry for their output. We obtain industry-level price information from the U.S. Bureau of Labor Statistics (BLS), using the producer price indices (PPIs) that they develop on each industry through a process of systematic sampling within industries (BLS, 2016). We obtain PPIs in their nominal form and apply a natural log transformation, following Pelztman (2000).

[2] https://www.census.gov/econ/concentration.html

[3] An alternative source, Compustat data is a common alternative to U.S. Census Bureau's concentration measure. However, it only accounts for public firms and correlates at a mere 13% with the Census Bureau's data, which is considered highly reliable (Ali et al., 2009).

[4] This follows how industry-level data on firm size is reported by the U.S. Census Bureau. The U.S. Small Business Administration (SBA) assigns various size standards to industries to classify businesses as "small" under its programs, and SBA standards may be based on revenues or number of employees, the latter of which may differ from 500 (although a threshold of 500 employees is common).

[5] https://www.census.gov/programs-surveys/susb.html

Controls

We include three controls to account for potentially confounding effects from other variables. First, we control for market competitiveness, as the average number of offers received by federal purchasers in response to solicitations within an industry, and at a given measurement occasion. Data on the number of offers received was collected from FPDS-NG. Specifically, the COMPETITIVENESS measure reflects the average number of offers received on RFPs that resulted in purchases. If no offers were received and thus no purchase was made, then the data would not be included within the dataset. However, if an RFP was later re-issued (which would typically be the case, possibly in some modified form) and resulted in a purchase, then the data would be included within the dataset. We control for competitiveness because it may be related to contract price and several of our explanatory variables, including industry concentration, thus posing a potential confound. Second, we account for growth in federal participation in markets for goods manufactured by an industry by including a control for the number of new contract awards within an industry, and at a given measurement occasion. Data on PARTICIPATION was also collected from FPDS-NG and is measured as the count of new contracts awarded by the federal government for goods manufactured by an industry. However, as this count of awards alone may not fully account for the nature of federal participation in markets, we include an additional control variable, OBLIGATIONS, which measures the total contractual obligations by the federal government on new contracts awarded by the federal government for goods manufactured by an industry. All three variables were log-transformed to reduce the effects of extreme values (positive skew) and to improve interpretability of regression coefficients.

Matching by Propensity Score

To further guard against potential confounds, we use propensity score matching to pair the 20 industries receiving a non-manufacturer rule waiver ("treatment") during the nine-year period with a similar set of industries who did not, thus creating an artificial control group. Propensity score matching is a technique commonly used to reduce exposure to potential confounds in settings characterized by non-randomized assignment or self-selection on one or more treatment conditions (Rosenbaum & Rubin, 1983). Wangenheim and Bayón (2007) provide a detailed description of the propensity score matching process. A logistic regression of TREATMENT on a series of covariates including a count of pre-existing non-manufacturer rule waivers, small business obligations, and initial level of industry concentration was estimated using data from the year 2007. As 2007 is the first year in our sample, it reflects the initial conditions for the industries at the start of our analysis. The logit model fit significantly better to the data than did its null alternative ($X_{\Delta}^{2}(4) = 20.11, p < .01$). To identify matches, we utilize caliper matching (Althauser & Rubin, 1970) with a tolerance of .20 of the standard deviation of the propensity score, following the recommendations of Austin (2011). We match industries without replacement with the objective of improving the precision of modeling results (Dehejia & Wahba, 2002). Each of the 20 industries receiving treatment in our dataset successfully matched to a similar, non-treated industry, thus resulting in a balanced sample of 40 industries. As we have nine annual observations on each industry, out total sample size is 360. Descriptive statistics and correlations for the resulting dataset are listed within Table 1.

Table 1. Correlation Matrix and Descriptive Statistics

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1. UTILIZATION	1.000							
2. TREATMENT	-0.191	1.000						
3. CONCENTRATION	0.145	0.034	1.000					
4. SMALLPROP	-0.112	0.147	0.235	1.000				
5. PRICEINDEX	0.146	-0.050	0.094	-0.167	1.000			
6. COMPETITIVENESS	0.030	0.011	0.100	0.161	0.112	1.000		
7. PARTICIPATION	-0.433	0.165	0.102	0.169	0.012	-0.024	1.000	
8. OBLIGATIONS	-0.740	0.204	-0.001	0.300	-0.105	-0.074	0.641	1.000
Mean	0.446	0.317	5.149	0.776	5.014	1.668	7.635	18.840
Standard Deviation	0.242	0.466	1.176	0.166	0.413	1.216	1.448	1.861
Minimum	0.022	0.000	0.693	0.163	3.619	-1.611	3.497	13.314
Maximum	0.998	1.000	6.172	0.991	5.779	6.458	11.265	23.021

Model and Methodology

A model of federal utilization of small businesses concerns as a function of class non-manufacturer rule waiver treatments is given in Equation 1.

$$\begin{aligned} UTILIZATION_{it} = {} & \beta_0 + \beta_1 \times TREATMENT_{it} \\ & + \beta_2 \times CONCENTRATION_i + \beta_3 \times CONCENTRATION_i \times TREATMENT_{it} \\ & + \beta_4 \times SMALLPROP_{it} + \beta_5 \times SMALLPROP_{it} \times TREATMENT_{it} \\ & + \beta_6 \times PRICEINDEX_{it} + \beta_7 \times PRICEINDEX_{it} \times TREATMENT_{it} \\ & + \beta_8 \times COMPETITIVENESS_{it} + \beta_9 \times PARTICIPATION_{it} \\ & + \beta_{10} \times OBLIGATIONS_{it} + e \end{aligned} \tag{1}$$

Given that the dependent variable is a proportion (a fraction) and is bounded between values of zero and one, estimation of the model using ordinary least squares can result in the prediction of values outside of the (0,1) interval (Papke & Wooldridge, 1996). Further, residuals produced from an ordinary least squares regression are unlikely to meet the assumptions of homogeneity and, thus, bias is likely in standard errors under the ordinary least squares estimator (Cohen et al., 2003, p. 240). Smith and Fernandez (2010) provide a discussion of this issue in the context of modeling small business utilization proportions, and identify several potential solutions, including the use of a quasi-maximum likelihood estimation technique developed by Papke and Wooldridge (1996). We also adopt this approach, but utilize the extension of the technique proposed by Papke and Wooldridge (2008) for estimating fractional response models with panel data, a Bernoulli quasi-MLE (QMLE) estimator (Papke & Wooldridge, 2008). Explanatory variables in QLME are specified as (1, $\mathbf{X}_{it}, \bar{\mathbf{X}}_i$) (Papke & Wooldridge, 2008, p. 124). As our interest is in change over time in the fractional response (i.e., the within-variance component), we limit our presentation of QLME results to those given by $\mathbf{X}_{it}$.

Results

Model estimation was performed in R (R Core Team, 2018). Estimates are presented in Table 2 and have been rescaled following the procedure given by Papke and Wooldridge (2008, Equation 3.11). As previously discussed, all three moderator variables (CONCENTRATION, SMALLPROP, PRICEINDEX) were centered about their grand means prior to entry into the regression equation. Thus, the coefficient for the non-manufacturer rule waiver treatment, TREATMENT, reflects the model-estimated effect of a waiver issuance at average levels of industry concentration, when the proportion of small firms in this industry is average, and at average prices. At this point, the simple effect (simple slope) of the waiver treatment is not decidedly non-zero (β* = .036, t = 1.704, p = .088).

Table 2. Regression Results

Explanatory Variable	Estimate	Unscaled	Std. Error	*t*-value	Pr(>|t|)
TREATMENT	0.036	0.098	0.058	1.704	0.088 *
CONCENTRATION × TREATMENT	-0.040	-0.123	0.047	-2.684	0.007 **
SMALLPROP	0.305	0.875	1.458	0.600	0.549
SMALLPROP × TREATMENT	0.046	0.231	0.268	0.860	0.390
PRICEINDEX	0.050	0.130	0.289	0.449	0.653
PRICEINDEX × TREATMENT	-0.106	-0.320	0.153	-2.095	0.036 **
COMPETITIVENESS (*control*)	-0.023	-0.066	0.033	-2.017	0.044 **
PARTICIPATION (*control*)	0.036	0.092	0.045	2.057	0.040 **
OBLIGATIONS (*control*)	-0.056	-0.153	0.083	-1.844	0.065 *

Notes. *p<.10, **p<.05. CONCENTRATION, SMALLPROP, AND PRICEINDEX are grand-mean centered.

Consistent with the expectations of Hypothesis 1, industry concentration (CONCENTRATION) has a statistically significant and negative moderating effect on the waiver treatment (*t* = -2.684, p < .01). Figure 1 depicts this interaction, providing simple slopes for the effect of the waiver treatment on small business utilization at high and low values of industry concentrations (± one standard deviation from the mean). Estimates and standard errors for the simple slopes were calculated using the mean vector and variance-covariance matrix for the model-implied coefficients (Spiller et al., 2013). When industry concentration is low, the waiver treatment has a positive and statistically significant effect on small business utilization (β* = .085, t = 2.876, p = .004). However, when industry concentration is high, the waiver has no discernable impact on small business utilization (β* = -.017, t = -.675, p = .500).

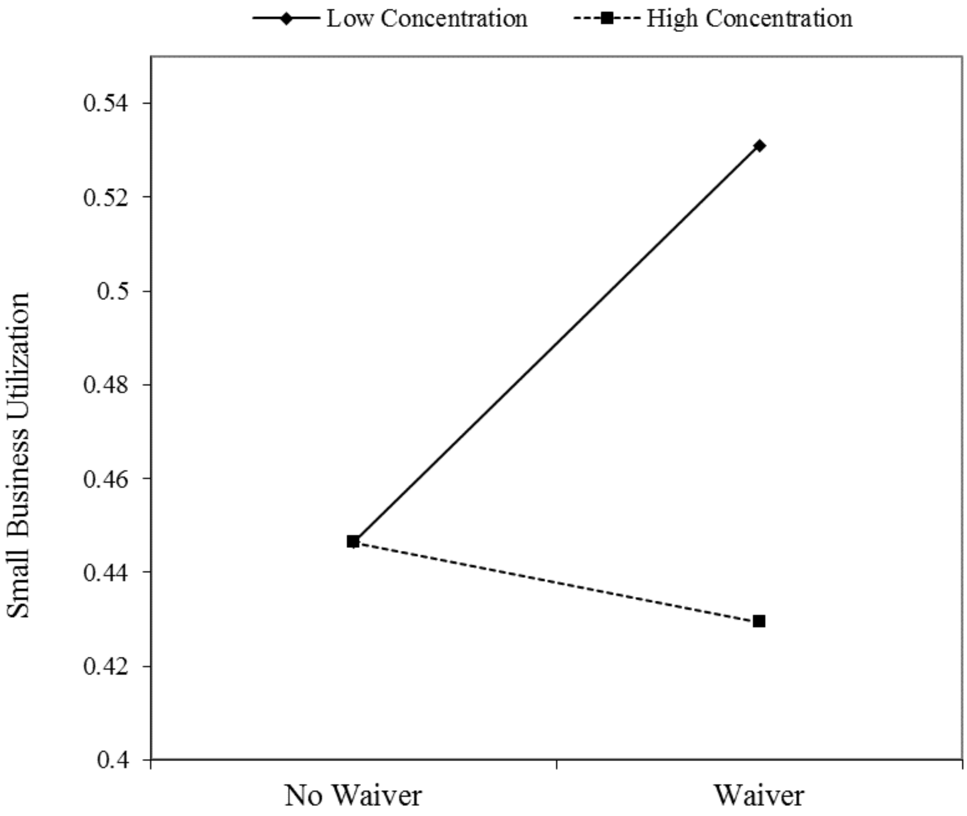


Figure 1. **. Interaction Plot of CONCENTRATION and Non-Manufacturer Rule Waiver Treatment**

The statistical model offered no support for Hypotheses 2, which suggested that the proportion of small firms in the industry (SMALLPROP) would amplify the effect of the waiver treatment. While the coefficient estimate for the interaction term was indeed positive, there was insufficient evidence to conclude that the effect exists (i.e., differs from a value of zero) in the population (β* = .046, t = .860, p = .390).

Hypothesis 3 was supported by the model. This hypothesis suggested that a waiver treatment would be less effective for industries experiencing high levels of price growth (PRICEINDEX). This implies a negative coefficient for the interaction term, as was estimated by the model (β* = -.106, t = -2.095, p = .036). The resulting interaction is depicted within Figure 2. When the industry price index (PPI) is low, the waiver treatment has a significant and positive effect on small business utilization (β* = .079, t = 2.657, p = .008). However, when the industry price index (PPI) is high, the effectiveness of the waiver treatment is attenuated, and does not appear to differ from a value of zero in the population (β* = -.012, t = -.406, p = .685).

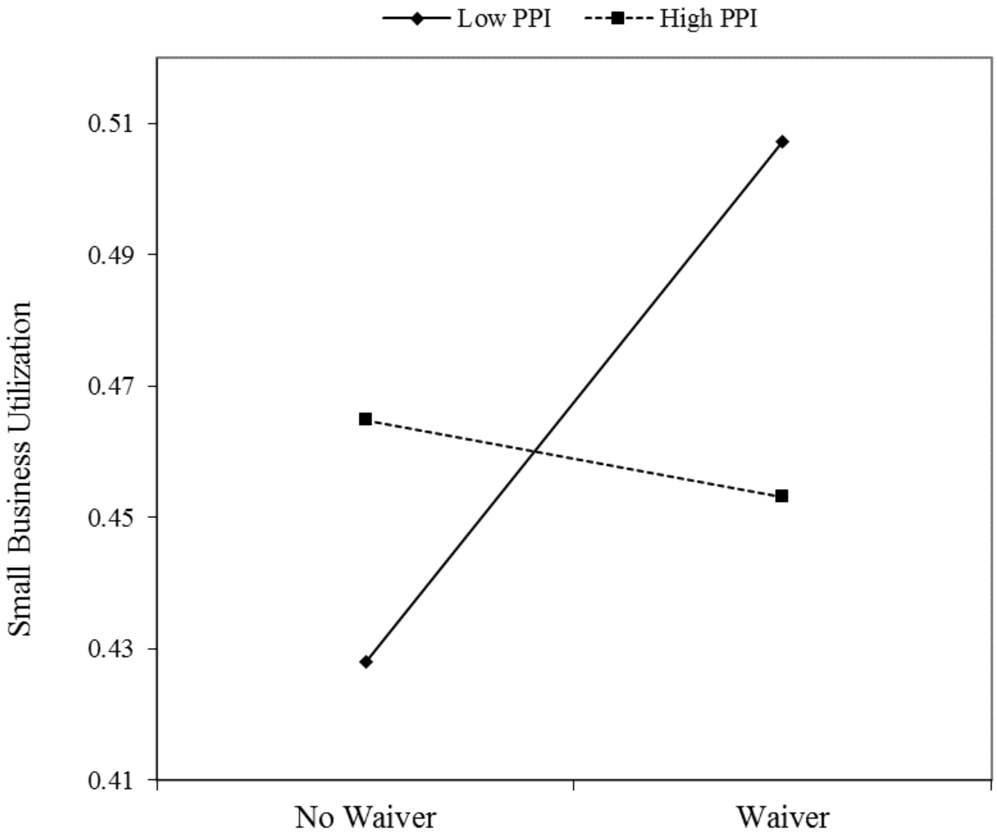


Figure 2. **Interaction Plot of PRICEINDEX (PPI) and Non-Manufacturer Rule Waiver Treatment**

Discussion

This is the first study that we are aware of to examine, using empirical data, industry-level conditions that amplify or attenuate the effectiveness of non-mandatory small business programs, such as class waiver program for the non-manufacturer rule. The study also provides a unique context to study the efficacy of marketing channel designs under differing industry conditions.

Our analysis demonstrates that industry-level factors strongly condition the effectiveness of class waivers to the non-manufacturing rule. For the "average" industry (e.g., as a measured by concentration, price levels, and the proportion of small firms in the industry), a class waiver may have little influence alone on small business utilization. This finding is not entirely surprising, given that the waivers are meant to be exceptions, and thus should not be expected to perform well in a general case (i.e., under general industry conditions). Yet, under the correct industry conditions, the waivers appear to have a robust, positive impact on small business outcomes. These conditions are discussed next.

The statistical results for our first hypothesis point to the criticality of industry composition to the efficacy of class waivers and, more broadly, to the success of targeted small business policies and programs. We found that, when industry concentration was high, issuance of a class waiver had no impact on the utilization of small businesses. Yet, when industry concentration is low, a waiver can produce a marked increase in small business utilization. Clearly, this result does not imply that the U.S. Small Business Administration should adopt a practice of broadly issuing class waivers within low-concentration industries. It does imply, however, that regulators and policy makers should consider the conditions present in the industry within the review and decision-making process for waiver issue: Low concentration can catalyze the waivers' effects. If concentration in an industry is high, then regulators might instead seek alternative mechanisms to spur small business growth and development, such as through bonding and funding programs.

Similarly, our results suggest that price stability—and the avoidance of high levels of industry price inflation—is critical to the success of the class waiver program. High industry-level prices nullified the positive effect that a class waiver to the non-manufacturer rule might otherwise have on small business utilization. There are two potential explanations for this. First, transaction costs between channel partners tend to rise as instability and uncertainty increases. Not only might quantities of final demand be more uncertain, but channel members may be incentivized to alter ordering and inventory behavior, reducing the potential for up-stream channel members to capitalize on potential economies in production and logistics. If additional transaction costs accrue between manufacturers and resellers (e.g., wholesalers, retailers), then pricing through indirect channels may become less competitive. Further, when prices are on the rise, buyers looking to enter into medium or long-term relationships for a class of products may be less willing to pay for value-added services provided by channel partners (e.g., local post-sales support), given the risk of future price increases.

Lastly, counter to our expectations, the data did not offer support for an amplification of the class waiver's effect when industries were comprised of a high proportion of small firms. However, this absence of an effect may not be entirely surprising. On one extreme, a waiver could not be expected to fare well at increasing small business utilization in an industry devoid of small businesses. On the other extreme, an industry that is already highly saturated with small business may already experience high levels of utilization, and thus the marginal benefit of a waiver may be minimal. For this reason, the relationship may truly be a polynomial (e.g., a quadratic and inverted-U), such that the waivers effects are greatest when there is only a moderate proportion of small businesses operating within the industry. While we were unable to test this proposition with our data, we discuss it as an area for future research.

Implications for Practice

Government procurement leaders who seek to maximize all tools at their disposal in order to comply by laws that facilitate small business participation may be disappointed to discover that factors beyond their control may render waivers an impotent tool. This suggests that procurement leaders should first conduct market analysis of industry factors; a basic understanding of the economic and environmental conditions can augment the effectiveness of waivers, where they are effective.

Waivers are least effective in industries characterized by high concentration and high price inflation, conditions that pose other procurement challenges. Knowing this, procurement managers who are forewarned of industry conditions can develop strategies appropriate to the industry and purchase circumstances. One could cite the success of specific examples of federal procurement initiatives that exhibit this approach, such as DIUx. DIUx caters to specific product-market-industry characteristics—perhaps offices specialized by purchasing circumstances would be appropriate for certain other industries.

Procurement managers might also consider the broader competitive and innovative benefits of providing certain resources to small businesses. Small businesses may suffer due to higher transaction costs relative to large businesses. At the individual business level, transaction costs for small businesses are usually lower (c.f., Paparoidamis et al., forthcoming), although purchase volume often would drive the use of many small businesses, for a greater sum of transaction costs than results from open market purchases from another large business. Facilitating inter-company information flows may be a strategy that re-empowers the NMR waiver so that it improves small business engagement.

Implications for Theory

Transaction costs enjoy an ample and well-established body of research with regard to government policies, yet relatively few studies connect transaction costs with channel design considerations in the context of government procurement. Environmental factors such as industry concentration and inflationary conditions may comprise the single most important consideration for the success of government initiatives to support small businesses, and these findings suggest that research should consider further moderator effects of environmental factors on government procurement policies. High industry concentration seemed to diminish the positive effects of waivers on small business, which may result from the relatively low transaction costs for large transactions among few large enterprises in highly concentrated industries, suggesting a primary role for transaction costs as an explanatory theory, at least for endogenous variables.

On the other hand, Coase (1937) originally proposed that the limit of the firm will occur where marginal transaction ("buy") costs will just balance marginal production ("make") costs, so it may be that exogenous variables related to industry structural factors ultimately determine production and transaction costs. For example, technological and product life-cycle maturity may determine the degree of industry concentration and its subsequent effects on small business participation. Our results provide evidence for the importance of structural factors. To address this structural difference between industries with regard to the effectiveness of waivers, transaction cost theory suggests that publicly funded information exchange networks may reduce transaction costs for small businesses in order generate the same waiver benefits for high concentration industries as for low. Institutional theory may offer an alternative both as an explanation and a remedy, suggesting that the social and regulatory environment surrounding highly concentrated industries may explain the difference in waiver outcomes, while simultaneously providing an example to emulate. Specifically, one-size-fits-all approaches to encourage small business participation may be infeasible, and tailoring of institutions may yield greater returns (Rodríguez-Pose, 2013).

Considering that traditional approaches have failed to resolve entirely the issue of sufficient federal procurement engagement with small business, new theory should be considered. Since small business policy is based in part upon creating healthier, more resilient, and more innovative economies, endogenous growth theory and the knowledge spillover theory of entrepreneurship may offer perspectives to study small business waivers that could explain our findings while providing guidance to public policy (c.f., Huggins & Thompson, 2015).

Study Limitations

This study has several limitations that should be kept in mind. A primary limitation, and one that we share with other research utilizing archival data, is that we are unable to directly observe or measure mechanisms that we theorize to underlie effects. Indeed, while we believe the theory and mechanisms that we rely on to be plausible, we are unable to conclude through our data or statistical analysis that these are truly the mechanisms that are at work and that our specification is indeed “correct” (Cudeck & Henly, 1991). Second, as data is not available on the issuance of individual (vs. class) waivers to the non-manufacturing rule, we are unable to control for the role that these waivers might have on promoting small business utilization. It seems likely, for instance, that industries most conducive to requests and approvals of individual waivers would also be most conducive to requests for class waivers.

Future Research Directions

Class NMR waivers usually originate from small business intermediaries who want to be eligible for somewhat restricted markets (small businesses only via set-asides). Future research could explore instances in which the buying agency originates the NMR waiver (i.e., an “individual” waiver) with the goals to understand (1) the circumstances in which this occurs, and (2) why it does not occur more often. Government buyers often do not conduct effective market research (Pang, 2018) and demonstrate a lack of commitment to small business goals (Hawkins, Gravier, & Randall, 2018).

Reference

Albano, G. L., Antellini Russo, F., Castaldi, G., & Zampino, R. (2015, October). Evaluating small businesses’ performance in public e-procurement: Evidence from the Italian government’s e-marketplace. *Journal of Small Business Management, 53*(Supplement), 229–250.

Ali, A., Klasa, S., & Yeung, E. (2009). The limitations of industry concentration measures constructed with Compustat data. *The Review of Financial Studies*, *22*(10), 3839–3871.

Althauser, R. P., & Rubin, D. (1970). *Selection and regression to the mean: Two hazards of matched sampling in non-experimental research*. Mimeographed. Princeton, NJ: Princeton University.

Audretsch, D. B. (2007). *The entrepreneurial society*. Oxford, England: Oxford University Press.

Audretsch, D. B., Keilbach, M. C., & Lehmann, E. E. (2006). *Entrepreneurship and economic growth*. Oxford, England: Oxford University Press.

Austin, P. C. (2011). An introduction to propensity score methods for reducing the effects of confounding in observational studies. *Multivariate Behavioral Research*, *46*(3), 399–424.

Carter, C. R., Auskalnis, R. J., & Ketchum, C. L. (1999). Purchasing from minority business enterprises: Key success factors. *Journal of Supply Chain Management, 35*(1), 28–32.

Chabowski, B. R., Hult, G. T. M., & Mena, J. A. (2011). The retailing literature as a basis for franchising research: Using intellectual structure to advance theory. *Journal of Retailing, 87*(3), 269–284.

Chiang, W.-y. K., Chhajed, D., & Hess, J. D. (2003). Direct marketing, indirect profits: A strategic analysis of dual-channel supply-chain design. *Management Science, 49*(1), 1–20.

Coase, R. H. (1937). The nature of the firm. *Economica*, 4(16), 386–405.

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2003). *Applied multiple regression/correlation analysis for the behavioral sciences*. Mahwah, NJ: Lawrence Erlbaum Associates.

Cudeck, R., & Henly, S. J. (1991). Model selection in covariance structures analysis and the “problem” of sample size: A clarification. *Psychological Bulletin*, *109*(3), 512.

Cullen, A. M. (2012). The small business set-aside program: Where achievement means consistently failing to meet small business contracting goals. *Public Contract Law Journal, 41*(3), 703–720.

Dehejia, R. H., & Wahba, S. (2002). Propensity score-matching methods for nonexperimental causal studies. *Review of Economics and Statistics*, *84*(1), 151–161.

Denes, T. A. (1997). Do small business set-asides increase the cost of government contracting? *Public Administration Review, 57*(5), 441–444.

Ellram, L. M., Tate, W. L., & Carter, C. R. (2007). Product-process-supply chain: An integrative approach to three-dimensional concurrent engineering. *International Journal of Physical Distribution & Logistics Management, 37*(4), 305–330.

Erdem, G., Kotzab, H., Teller, C., Yumurtaci Hüseyinoglu Isik, Ö., & Pöppelbuß, J. (2018). Omni-channel retailing research—State of the art and intellectual foundation. *International Journal of Physical Distribution & Logistics Management, 48*(4), 365–390.

Federal Procurement Data System–Next Generation (FPDS-NG).

Federal Procurement Data System. (2005). Small business goaling reports. Retrieved June 1, 2016, from https://www.fpds.gov/fpdsng_cms/index.php/en/reports.html

Federal Procurement Data System. (2006). Small business goaling reports. Retrieved June 1, 2016, from https://www.fpds.gov/fpdsng_cms/index.php/en/reports.html

Federal Procurement Data System. (2007). Small business goaling reports. Retrieved June 1, 2016, from https://www.fpds.gov/fpdsng_cms/index.php/en/reports.html

Federal Procurement Data System. (2008). Small business goaling reports. Retrieved June 1, 2016, from https://www.fpds.gov/fpdsng_cms/index.php/en/reports.html

Federal Procurement Data System. (2009). Small business goaling reports. Retrieved June 1, 2016, from https://www.fpds.gov/fpdsng_cms/index.php/en/reports.html

Federal Procurement Data System. (2010). Small business goaling reports. Retrieved June 1, 2016, from https://www.fpds.gov/fpdsng_cms/index.php/en/reports.html

Federal Procurement Data System. (2011). Small business goaling reports. Retrieved June 1, 2016, from https://www.fpds.gov/fpdsng_cms/index.php/en/reports.html

Federal Procurement Data System. (2012). Small business goaling reports. Retrieved June 1, 2016, from https://www.fpds.gov/fpdsng_cms/index.php/en/reports.html

Federal Procurement Data System. (2013). Small business goaling reports. Retrieved June 1, 2016, from https://www.fpds.gov/fpdsng_cms/index.php/en/reports.html

Federal Procurement Data System. (2014). Small business goaling reports. Retrieved June 1, 2016, from https://www.fpds.gov/fpdsng_cms/index.php/en/reports.html

Federal Procurement Data System. (2015). Small business goaling reports. Retrieved June 1, 2016, from https://www.fpds.gov/fpdsng_cms/index.php/en/reports.html

Grammich, C. A., Edison, T., Moore, N. Y., & Keating, E. G. (2011). *Small business and defense acquisitions: A review of policies and current practices*. Santa Monica, CA: RAND Corporation, National Defense Research Institute.

Hawkins, T., Gravier, M., & Randall, W. (2018). Socio-economic sourcing: Benefits of small business set-asides in public procurement. *Journal of Public Procurement, 18*(4), 217–239.

Head, B., & Kirchhoff, B. The growth, decline and survival of small businesses: An exploratory study of life cycles. *Journal of Small Business Management*, *47*(4), 531–550.

Huggins, R., & Thompson, P. (2015). Entrepreneurship, innovation and regional growth: A network theory. *Small Business Economics*, 45(1), 103–128.

Ingene, C. A., & Parry, M. E. (1995). Channel coordination when retailers compete. *Marketing Science (1986–1998), 14*(4), 360.

Krafft, M., Goetz, O., Mantrala, M., Sotgiu, F., & Tillmanns, S. (2015). The evolution of marketing channel research domains and methodologies: An integrative review and future directions. *Journal of Retailing, 91*(4), 569–585. doi:http://dx.doi.org/10.1016/j.jretai.2015.05.001

Krause, D. R. (1997). Supplier development: Current practices and outcomes. *International Journal of Purchasing and Materials Management, 33*(2), 12–19.

Lewis, G. H. (2017). Effects of federal socioeconomic contracting preferences. *Small Business Economics*, *49*, 763–783.

Logožar, K. (2013). The specifics of supply chain integration with small and medium-sized enterprises. *Our Economy (Nase Gospodarstvo)*, *59*.

Pang, S. H. (2018). *Critical issues in the Air Force medical equipment procurement process* (No. AFIT-ENS-MS-18-M-153). Wright-Patterson AFB, OH: Air Force Institute of Technology.

Paparoidamis, N. G., Katsikeas, C. S., & Chumpitaz, R. (forthcoming). The role of supplier performance in building customer trust and loyalty: A cross-country examination. *Industrial Marketing Management*.

Papke, L. E., & Wooldridge, J. M. (1996). Econometric methods for fractional response variables with an application to 401(k) plan participation rates. *Journal of Applied Econometrics*, *11*(6), 619–632.

Papke, L. E., & Wooldridge, J. M. (2008). Panel data methods for fractional response variables with an application to test pass rates. *Journal of Econometrics*, *145*, 121–133.

Parker, G. G., & Anderson, E. G., Jr. (2002). From buyer to integrator: The transformation of the supply-chain manager in the vertically disintegrating firm. *Production and Operations Management, 11*(1), 75–91.

Peltzman, S. (2000). Prices rise faster than they fall. *Journal of Political Economy*, *108*(3), 466–502.

Qi, Z., Hong, L., & Xiaoxiao, Q. (2014). Research on small and medium enterprises financing mode based on supply chain finance. *Journal of Chemical & Pharmaceutical Research, 6*(5), 1818–1824.

R Core Team. (2018). R: A language and environment for statistical computing. Vienna, Austria: R Foundation for Statistical Computing. Retrieved from https://www.R-project.org/

Ram, M., & D. Smallbone. (2003). Supplier diversity initiatives and the diversification of ethnic minority businesses in the UK. *Policy Studies, 24*(4), 187–204.

Robbins, D. K., Pantuosco, L. J., Parker, D. F., & Fuller, B. K. (2000). An empirical assessment of the contribution of small business employment to U. S. state economic performance. *Small Business Economics, 15*(4), 293–302.

Rodríguez-Pose, A. (2013). Do institutions matter for regional development? *Regional Studies*, *47*(7), 1034–1047.

Rosenbaum, P. R., & Rubin, D. B. (1983). The central role of the propensity score in observational studies for causal effects. *Biometrika*, *70*(1), 41–55.

Sakallaris, A.G. (2007). Questioning the sacred cow: Reexamining the justifications for small business set asides. *Public Contract Law Journal*, *36*(4), 685–700.

Smith, C. R., & Fernandez, S. (2010). Equity in federal contracting: Examining the link between minority representation and federal procurement decisions. *Public Administration Review*, 70(1), 87–96.

Spence, L. J., & Lozano, J. F. (2000). Communicating about ethics with small firms: Experiences from the U.K. and Spain. *Journal of Business Ethics, 27*(1/2), 43–53.

Sperling, G. B., & Mills, K. G. (2012). *Moving America's small businesses & entrepreneurs forward: Creating an economy built to last*. Washington, DC: National Economic Council, The White House.

Spiller, S. A., Fitzsimons, G. J., Lynch, J. G., Jr., & McClelland, G. H. (2013). Spotlights, floodlights, and the magic number zero: Simple effects tests in moderated regression. *Journal of Marketing Research*, 50(2), 277–288.

Thurik, R., & Wennekers, S. (2004). Entrepreneurship, small business and economic growth. *Journal of Small Business and Enterprise Development, 11*(1), 140–149.

U.S. Bureau of Labor Statistics. (2016). Producer price indices. *In Handbook of methods* (Ch. 14). Washington, DC: Author.

U.S. Small Business Administration. (2012). *Small business economy 2012*. Retrieved from https://www.sba.gov/sites/default/files/files/Small_Business_Economy_2012(2).pdf

U.S. Small Business Administration. (2018). *Small business economic profiles 2018*. Retrieved from https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf

Vinhas, A.S., Chetterjee, S., Dutta, S., Fein, A., Lajos, J., Neslin, L., Ross, W., & Wang, Q. (2010). Channel design, coordination, and performance: Future research directions. *Marketing Letters*, *21*(3), 223–237.

Walker, H., & Preuss, L. (2008). Fostering sustainability through sourcing from small businesses: Public sector perspectives. *Journal of Cleaner Production,* 16(15), 1600–1609.

Wangenheim, F. V., & Bayón, T. (2007). Behavioral consequences of overbooking service capacity. *Journal of Marketing*, *71*(4), 36–47.

Wennekers, S., & Thurik, R. (1999). Linking entrepreneurship and economic growth. *Small Business Economics, 13*(1), 27–56.

Winsor, R. D., Manolis, C., Kaufmann, P. J., & Kashyap, V. (2012). Manifest conflict and conflict aftermath in franchise systems: A 10-year examination. *Journal of Small Business Management*, *50*(4), 621–651.

Yoshida, K., & Deyle, R.E. (2005). Determinants of small business hazard mitigation. *Natural Hazards Review, 6*(1), 1–12.

Young, J. A., & Merritt, N. J. (2013). Marketing channels: A content analysis of recent research, 2010–2012. *Journal of Marketing Channels, 20*(3/4), 224–238.

Commercial Aircraft Pricing: Models, Applications, and Lessons Learned

Bruce Harmon—works for the Institute for Defense Analyses (IDA), where he has been a professional Research Staff Member for over 30 years. Harmon has extensive experience modeling the costs and schedules of various aerospace systems, as well as performing analyses of other acquisition issues. He is a PhD candidate in economics at American University in Washington, DC. [bharmon@ida.org]

Abstract

The procurement of commercial items presents both opportunities and challenges for the Department of Defense. Among the challenges is the negotiation of “fair and reasonable” prices with suppliers where competitive sources are not relevant. This paper presents analyses to address this challenge for commercial aircraft that serve as the basis for military systems. Using insights from the economics literature on aspects of the commercial aircraft market, we develop estimating models for aircraft price that take into account both supply and demand drivers, across both aircraft models and time. These models are applied to the KC-46A airborne tanker program, prices of which are subject to negotiation. Other factors affecting the commercial aircraft market and aircraft used in these programs (Boeing variants) are also addressed. Lessons learned applicable to the general problem of negotiation of contracts for commercial items are enumerated.

Background

The procurement of commercial items presents both opportunities and challenges for the Department of Defense (DoD). Among the challenges is the negotiation of “fair and reasonable” prices with suppliers where competitive sources do not exist. The Institute for Defense Analyses (IDA) has performed a series of studies developing estimating relationships for the prices of commercial aircraft, variants of which figure in DoD acquisition programs (Harmon, Sullivan, & Davis, 2010). Unlike in the case of purpose-built military aircraft, DoD negotiators generally do not have access to the underlying costs or cost estimating relationships derived from historical costs for analogous items. Buying commercial aircraft is substantially different from buying military aircraft or commodity items from other types of commercial suppliers. Lessons learned from this past rese   arch can help inform current Air Force negotiations on the prices of current and future systems; of particular interest is the KC-46A program. The lessons learned also have implications for the broader portfolio of the DoD’s commercial items purchases, particularly those bought in thin markets, and/or markets dominated by sellers with market power where competitive sourcing is not relevant.

The Economics of the Commercial Aircraft Market

The market for commercial aircraft with a range greater than 3,000 nautical miles (NM) is currently a duopoly, with Boeing and Airbus the only producers. In a duopoly such as this, the participants have a degree of market power not evident in more competitive markets. The suppliers’ choice of quantity (price) has an effect on market price (quantity demanded), as each supplier contributes a large part to industry output. Also, given learning in the aircraft industry, the choice of quantity for a given time period affects costs in future time periods. This combination of attributes means that for any given product line and time period, price can be below marginal cost (startup period)[1] or above marginal cost (mature program). In addition, given market power (the supplier faces a downward sloping demand curve), price discrimination is also evident. This contrasts with a competitive market in which all firms are price takers; the cost of production for any given firm does not affect the market price. All of these factors contribute to the difficulty in arriving at fair and reasonable prices for commercial aircraft.

Overview of the Literature

These observations are drawn from substantial academic literature on the economics of the commercial aircraft industry, presented in Harmon et al. (2010), in which price determination is an important aspect of much of the research. This literature provides important insights regarding potential drivers of aircraft price levels and movements over time. These studies show that, although learning will not affect purchase price to the degree evident in a contracting environment—as in the military aircraft procurement, where prices are negotiated based on cost—there still can be some effect (Baldwin & Krugman, 1988; Benkard, 2004; Irwin & Pavcnik, 2004). This should be true for anything that affects the cost structure of the industry or a given product line. For example, estimated price increases that followed the 1992 reduction in government subsidies were coincident with calculated increases in producer costs (Irwin & Pavcnik, 2004). Other possible cost drivers that could show up in price include labor productivity, secular trends, and cyclical movements. Some fixed costs will be “quasi-fixed”—portions of labor inputs that are sticky relative to production rate. This was noted in Kronemer and Henneberger (1993), a Bureau of Labor Statistics (BLS) study of labor productivity in the aircraft industry. The BLS found that labor productivity was highly procyclical—higher output measures were associated with higher productivity growth as quasi-fixed portions of labor were spread over more units. Their data also show a longer-term upward trend in labor productivity of 1.5% to 2.5% per year.

Modeling Approaches

The models of the aircraft industry presented in the economics literature have, by necessity, been abstracted from a complex reality. They have at least four things in common:

- Use of a multi-period dynamic framework;
- Rules guiding the strategic behavior of suppliers in a duopoly/oligopoly situation in which game-theoretic approaches are used to solve for industry equilibrium;
- Inclusion of learning curves in the supply functions of the firms, while taking into account the dynamic effects of learning on firm decisions; and
- Demand relations reflecting the derived demand of aircraft as an input to the production of air services.

All the models take the manufacturers as value maximizers over an extended time horizon where the value function is, assuming a homogeneous product, for firm *j*,

[1] Due to learning-by-doing, the first quantity produced has a very high cost. Prices in the startup period are usually observed to be below marginal costs.

$$V_j = \sum_{t=0}^{T} R^t (p_{jt} q_{jt} - c_{jt} q_{jt}), \qquad (1)$$

where *Vj* is the net present value for firm *j*, *R* is a discount factor and p_{jt}, q_{jt}, and c_{jt} are the relevant price, quantity, and marginal cost.[2] Modifications to this basic setup were made by the different researchers to reflect additional assumptions. The firms' strategic behavior is portrayed either as quantity setting (Cournot game) or price setting (Bertrand game). The choice of q_{jt} will affect both the current price through the demand relation, $p_{jt}=f(Q_{jt})$, where $Q_{jt} = \sum_{j=1}^{J} q_{jt}$, and current and future costs, through the learning curve. In the Bertrand game, choosing p_{jt} will affect q_{jt}, which in turn will affect future costs through the learning curve. The models vary in complexity and realism. For the simplest model, stated in Baldwin and Krugman (1988), a single-period equilibrium solution for market price (p_t) was determined as

$$p_t = \frac{c_t + z_t}{1 - (1\text{-}s) / E}, \qquad (2)$$

where c_t is the marginal cost of the aircraft, z_t is the shadow value of current production arising from reductions in future costs due to learning, *s* is the market share of the subject firm, and *E* is the demand elasticity ($E > 0$).[3]

Example Program: KC-46A

In the KC-46A program, government-funded development includes the creation of a new minor model of the 767, the 767-2C, which was not previously available to commercial customers. The 767-2C includes a combination of features available in other Boeing commercial aircraft, including freighter floors and doors, convertible passenger capability, an upgraded cockpit, and higher maximum take-off weight (MTOW). In addition, tanker mission system provisions are also incorporated; although these features were not available on previous Boeing commercial aircraft, they are "of a type" changes that commercial customers might specify (e.g., added provisions for non-standard buyer-furnished equipment [BFE]). Boeing has applied for a Federal Aviation Administration "amended type certificate" (ATC) for the 767-2C. Given the ATC, the 767-2C will be commercially available to other customers. All of these factors add challenges to the negotiation of fair and reasonable prices, as pricing history for direct commercial analogs do not exist. The effects of these challenges are mitigated by an acquisition strategy in which the initial competition between suppliers (resulting in the choice of Boeing over Airbus in February 2011) provided for price discovery. The award covered a Fixed-Price Incentive Firm contract for Engineering and Manufacturing Development along with Firm Fixed Price contract options for Low Rate

[2] The definition of marginal cost in most of this literature is not the cost of the last aircraft built during the time increment, but the $^{\text{average}}$ cost over that time period, implying the inclusion of recurring fixed costs.

[3] Denote demand with *x*. The price elasticity of demand is – $(\Delta x/\Delta p)\ (p/x)$, which measures the percentage change in demand in response to a 1% change in price.

Initial Production Lots 1 and 2, and Not-to-Exceed (NTE) contract options with an Economic Price Adjustment (EPA) clause for Full Rate Production Lots 3 through 13 (DoD, 2016). It is at Lot 3 (FY 2017) where negotiation becomes relevant.

Modeling Commercial Aircraft Prices

We use least-squares regression techniques to define and test specifications of the price estimating relationships. Prices are treated as dependent variables and related to independent variables, which we hypothesize to be price drivers. In the case of least-squares regressions, the functions are defined by parameter estimates on the independent variables, determined by minimizing the squared errors of the regression line from the actual data. The price estimating relationships take on the multiplicative form:

$$p_j = f(x_j, \beta) e^{u_j}, \tag{3}$$

where p_j is the value of the observed price for aircraft j, x_j is the vector of independent variables, □ is the vector of parameter estimates, and u_j is the error term. Without loss of generality, assume that the equation takes on the intrinsically linear form with an intercept, one regressor x_1 (price driver), and one dummy variable *D,*

$$p_j = \beta_o x_{1j}^{\beta_1} \beta_2^{D_j} e^{u_j}, \tag{4}$$

and then OLS regression techniques can be applicable. To do this, the equation is transformed to a log-log form:

$$\ln(p_j) = \ln(\beta_0) + \beta_1 \ln(x_{1j}) + \ln(\beta_2) D_j + u_j. \tag{5}$$

OLS will produce parameter estimates of $b_0 \equiv \ln(\beta_0)$, $b_1 \equiv \beta_1$, and $b_2 \equiv \ln(\beta_2)$. Both β_0 and β_2 can be recovered by taking an anti-logarithmic transformation of b_0 and b_2 (i.e., by calculating e^{b_0} and e^{b_2}). The parameter estimate b_1 has a natural interpretation of elasticity, measuring the percentage change in price with respect to a 1% change in x_1. The parameter b_2 represents a change in price ($\Delta p_j/p_j$) when the dummy variable switches its value from 0 to 1.

When describing the estimating relationships, information presented includes R^2, adjusted R^2, the standard error of the estimate ($\hat{\sigma}$), and the t-statistics (which are the ratios of the parameter estimates to their standard errors), as well as associated levels of statistical significance for each of the parameter estimates. We generally exclude variables whose parameter estimates are not significant at the 0.1 level, although some exceptions are made. In a linear model, R^2 measures the proportion of the total variance in the data explained by the model. Although this is not strictly true for most of our models because they are nonlinear, the R^2 analog provides useful information about the relative fit of the models. Adjusted R^2 presents this information adjusted for the number of independent variables in the regression. R^2 and adjusted R^2 are calculated from the data and model after they are transformed back from log space to arithmetic space. $\hat{\sigma}$ is calculated in log space; it can be converted into minus/plus percentages of price in the original space by calculating values for $\left(e^{-\hat{\sigma}}\right) - 1$ and $\left(e^{+\hat{\sigma}}\right) - 1$. Measures derived from the standard errors provide information regarding the uncertainty of the estimates.

Data

The IDA team used data from airline industry consultants to build price estimating relationships for commercial aircraft. Airlines and manufacturers withhold transaction price information from public release, and Department of Transportation transaction price data for contemporary experience are not available. Although list prices are available on Boeing and Airbus websites, aircraft are generally sold at a substantial discount from list. The airline consultants estimate prices for a variety of clients including aircraft purchasers, lessors, insurers, and investors. They are coy about their estimating methods; they seem to extrapolate from a limited number of actual data points (often from their clients) based on financial valuation models.

IDA's previous analysis of the KC-767 purchase price (Nelson et al., 2003) noted uncertainties associated with reported aircraft price data:

> The complexity of the transactions comes from two sources: the variation in content from one sale to another, and the nature of the contractual arrangements involved. Both sources of complexity make it difficult to interpret any known historical sales prices.
>
> The content included in a given sale may on the one hand include spare parts, training, and maintenance support. On the other hand, the sales price may not include buyer furnished equipment such as interiors, in-flight entertainment, seats and galleys. Additionally, 767 aircraft, like most commercial models, are sold with a wide range of features such as upgraded avionics, engines, fuel capacities, maximum gross takeoff weight and cargo handling systems.

This uncertainty was addressed for 767 pricing by collecting data from multiple sources, representing multiple years and transactions. This general strategy was expanded to the broader commercial aircraft market by statistically defining price estimating relationships. The goal was to abstract from the available data some reference value for a given aircraft model based on the consultants' pricing data, regardless of the conditions of specific transactions or possible measurement error associated with the individual data points used. The regression analyses employed generated the expected values of prices conditioned on measures of aircraft utility and other price drivers. The statistical analyses in turn provided measures of estimation error that partially reflect uncertainties in the data.

IDA price estimating research was first performed in 2009 to 2010 in Harmon et al. (2010) using data from Airline Monitor, AVITAS, and Morten Beyer & Agnew (MBA). These data included reported prices through 2009. The AVITAS and MBA data showed similar prices for the same aircraft model, while the Airline Monitor data showed consistently higher prices, particularly for wide-body (WB) aircraft. Also, Airline Monitor's time series data showed almost no price variability between years, and price data for discontinued aircraft models were reported after they ceased delivery. As AVITAS did not include time series data by aircraft model, we chose to update only the MBA data; the updated data used in modeling included reported prices through January 2016. MBA presented "Base Value" and "Current Market Price" data—in most cases the two values were the same, but when they were different, we used the Current Market Price value. Prices were for typical airline configurations, including interiors/BFE.

Table 2 shows the coverage by year for the MBA data used in the regression modeling. Note that there was a gap in data reporting in 2010 and 2011.

Table 2. Data Coverage

Manufacturer	Aircraft	Years in 2010 Study	Additional Years in 2016 Update
Airbus	A330-200	1998–2009	2012–2016
	A330-300	1996–2009	2012–2016
	A330-300F	NA	2014–2016
	A380-800	N/A	2012–2016
Boeing	737-600	1998–2006	N/A
	737-700	1998–2009	2012–2016
	737-800	1998–2009	2012–2016
	737-900	2001–2005	N/A
	737-900ER	2006–2009	2012–2016
	747-8	N/A	2012–2016
	747-F	N/A	2016
	767-200ER	1988–1991, 2000–2007	N/A
	767-300ER	1988–2009	2012–2013
	767-300F	NA	2014–2016
	767-400ER	2000–2002	N/A
	777-200	1995–2006	N/A
	777-200ER	1997–2009	2012–2014
	777-200LR	2007–2009	2012–2014
	777-300	1998–2006	NA
	777-300ER	2005–2009	2012–2016
	777F	NA	2014–2016
	787-8	N/A	2012–2014
	787-9	N/A	2016

All dollar amounts are measured in calendar year (CY) 2016 dollars. The inflation adjustment is made using the U.S. Gross Domestic Product (GDP) deflator as reported by the Bureau of Economic Analysis (BEA). The effect of other economic factors (fuel price, world GDP, cumulative aircraft quantity) are weighted based on estimates from panel data analyses that are described later.

Aircraft characteristics used as cost drivers in the regressions were open source data obtained primarily from the aircraft manufacturers' websites. Price drivers were aircraft characteristics fixed over time reflecting utility to airlines. Different independent variables and subsets of data were included in the resulting price estimating relationships. Either MTOW, Seats and Range (Seat Miles[4]), or Payload was used as the primary driver. These drivers are presented graphically for the aircraft in the data sample in Figure 1.

[4] Seat Miles is a measure of an aircraft's passenger-carrying capacity. It is equal to the number of seats available multiplied by the maximum range in miles.

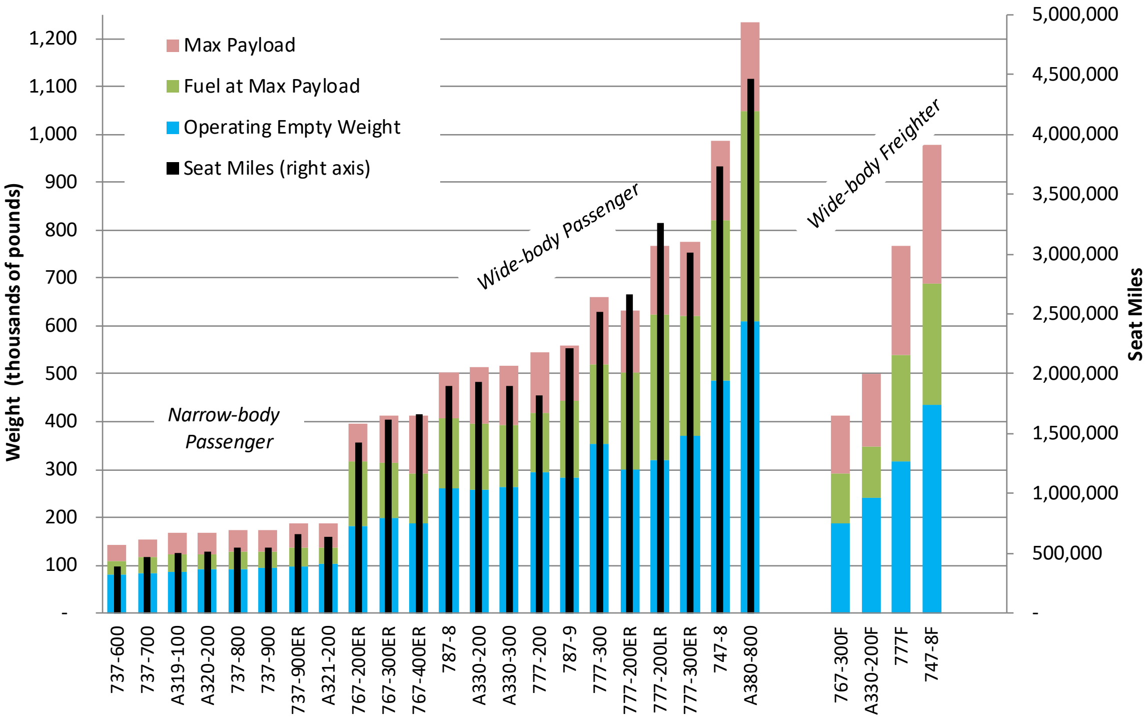


Figure 1. **MTOW and Seat Miles for Commercial Aircraft Sample**

Data can be further broken down by aircraft model. An aircraft model is introduced, manufactured, and phased out over time. Therefore, a given model is usually observed in multiple years over a specific range of years. Some drivers change over time and model. For example, the variables representing and measuring utility (demand) and cost (supply) affect prices over time. The economics literature informs our choice of independent variables.

Pooled OLS Models

Our data were a mix of cross-section (data by aircraft model) and time series (for a given model). The time series data sample included observations from 1988 to 2016, covering periods that vary by model; the data ranges are shown in Table 2. Our empirical regression took the logarithmic form:

$$p_{jt} = \mathbf{z}_j \alpha + \mathbf{x}_{jt} \beta + \varepsilon_{jt} \text{ ,} \tag{6}$$

where the *j* subscript indexed each model, $\mathbf{z}_j$ was a vector containing a constant term and variables for each model that are fixed over time, and $\boldsymbol{x}_{jt}$ was a vector of regressors that varied over model and time.

In terms of the price estimating model, the aircraft-model-specific variables fixed over time (e.g., Seat Miles and MTOW) were contained in $\mathbf{z}_j$, while the x_{jt}s were the economic variables that changed over time and model (including delivery quantities to capture learning). If the observed aircraft-characteristic variables fully define $\mathbf{z}_j$, then OLS can be used to estimate the model (Greene, 2002). Given positive diagnostics regarding $\mathbf{z}_j$, we chose to estimate the price estimating relationships using OLS.[5]

For the aircraft model-specific variables (the z_js) we found either Seats and Range or MTOW to be statistically significant. The MTOW specification allowed us to include freighter aircraft in the sample. The MTOW model showed a substantially better fit than the Seats and Range model. One reason for this may be the ambiguity regarding seating configurations for the passenger aircraft. We also tried different combinations and transformations of the constituents of MTOW (e.g., empty weight, weights for payload and fuel), but we found that MTOW fit the best. For the updated data sample, we did not find a freighter effect.

For the economic variables, we experimented with different time lags and forms of world GDP growth (International Monetary Fund, 2016), fuel prices (U.S. Energy Information Administration, n.d.), delivery rates, and aircraft cumulative quantity, as well as a time trend. As there were already substantial correlations between time, cumulative aircraft quantity, and fuel price, we used the de-trended series for GDP growth.

The net effect of market cycles on aircraft prices is an interesting empirical question. There is a supply-side argument that higher production rates would mean lower unit costs and prices.[6] The demand-side argument is that higher economic growth would raise the utility of aircraft to the airlines and prices would rise. Although these are two different effects, they were highly correlated with one another in the data. We found that higher GDP growth is associated with higher prices, and that measures of delivery rate were either statistically insignificant when entered with GDP growth or carried the same sign. In the end, we chose de-trended world real GDP growth, lagged two years, to capture the effect of market cycles on prices.

The impact of other x_{jt}s were not ambiguous, as the demand and supply/cost effects were more clearly delineated. Fuel price was a demand-side driver, where higher fuel prices were expected to result in lower aircraft prices. Higher cumulative quantities should result in lower costs and prices. Long-term increases in productivity should lead to lower real prices over time for a given aircraft capability.

For our preferred baseline pooled OLS regression, we identified five price drivers: maximum takeoff weight ($MTOW_j$), cumulative quantity ($CumQ\_L1_{jt}$), de-trended world real GDP growth rate ($WGDP\_L2_{jt}$), fuel price ($FuelP\_L1_{jt}$), and calendar year ($Year_{jt}$), each of which is measured as explained below:

- $MTOW_j$ is described above;
- $4Engines_j$ is a dummy taking *1* if model *j* is a four-engine aircraft and *0* if it is a two-engine aircraft*;*

[5] Although there was evidence in the regression results that assumptions required for OLS to be the best unbiased linear estimator were violated (unequal error variances across panels/heteroskedasticity and correlation of errors across time within each panel/serial correlation), we judged alternatives to address these problems (generalized least squares or the use of cluster robust standard errors) inappropriate, given our data sample.

[6] There were also offsetting supply-side arguments; production spikes may be associated with increased prices for inputs and increasing marginal costs.

- $CumQ\_L1_{jt}$ is the cumulative quantity for the aircraft family associated with aircraft model *j* at the end of the prior year;
- $WGDP\_L2_{jt}$ is world real GDP growth expressed as percentage deltas from the trend and lagged two years, where the trend is established using the Hodrick-Prescott filter (Hodrick & Prescott, 1997);
- $FuelP\_L1_{jt}$ is the real price of jet fuel lagged one year; and
- $Year_{jt}$ is the calendar year associated with each model *j* and time *t*.

When estimating the model, we included a dummy variable for WB aircraft, along with an interaction term with the $MTOW_i$ variable. This resulted in a unique slope coefficient on $MTOW_i$ as well as a different intercept for WB. This meant a separate model estimated for each of WB and narrow-body (NB) aircraft, as shown in the specification presented in **Error! Reference source not found.**. Variations on both the MTOW and Seat Miles pooled OLS models included production rate for each aircraft family as an additional independent variable. Our estimated models follow (standard errors are included under the parameter estimates):

- For WB aircraft:

$$ln(p_{jt}) = 13.01+1.147\ ln(MTOW_j)-0.253\ (4Engines_j) - 0.031\ ln(CumQ\_L1_{jt})$$

(.140) (.039) (.008)

$$+\ 1.371\ (WGDP\_L2_{jt}) - 0.038\ (FuelP\_L1_{jt}\ ) -0.011\ Year_{jt},$$

(.738) (.013) (.002)

- For NB aircraft, the interaction terms result in a unique intercept and MTOW coefficient, with the remaining coefficients remaining the same as for WB aircraft:

$$ln(p_{jt}) = 4.37 + 1.907\ ln(MTOW_j)$$

(.738)

Error! Reference source not found. compares MBA-reported data points to the projected prices using the estimated models.

$$p_{WB\,jt} = 447{,}111\ MTOW_j^{1.147}\ .777^{4Engine_j}\ CumQ\_L1_{jt}^{-.031}\ 1.371^{WGDPc\_L2_{jt}}\ 0.963^{FuelP\_L1_{jt}}\ 0.989^{Year_{jt}}$$

$$\left(p_{NB\,jt} = 79.4\ MTOW_j^{1.907}\right)$$

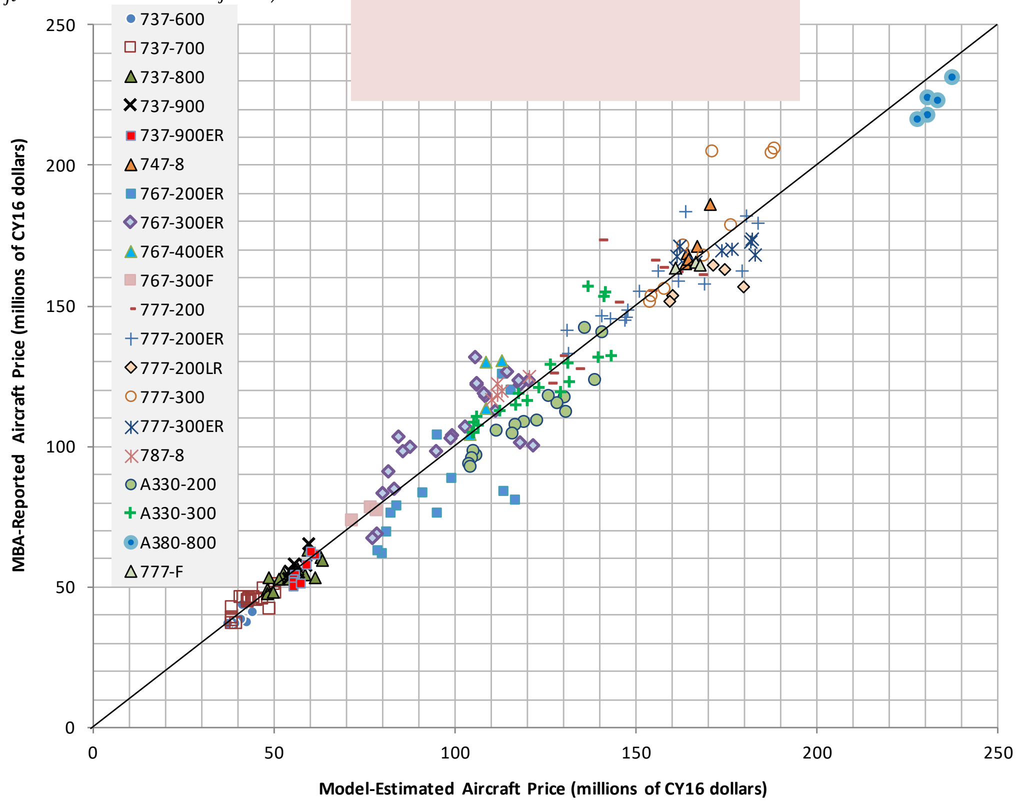


Figure 2. **MTOW Panel Data Model**

All of the parameter estimates for the preferred model shown in **Error! Reference source not found.** are significantly different from zero at *p* = .06 or better. Estimates for the coefficient on *CumQ_L1*$_{jt}$ indicate equivalent price improvement curve slopes of 97.9%. This is much shallower than typical cost improvement curves and is consistent with the economics literature. The estimates on *WGDP_L2*$_{jt}$ suggest that if world real GDP growth is 1 percentage point above trend two years prior to aircraft delivery (say, 4.4% versus the 3.4% growth trend estimated for 2017 using the Hodrick-Prescott filter), the price will be 1.4% higher than if GDP growth was at trend.

Estimates for the fuel price coefficients indicated that a $1 per gallon increase in fuel price one year prior to aircraft delivery results in a 3.8% decrease in price. The reasonableness of this estimate was tested by an approach similar to that taken in Markish (2002), where changes in fuel costs were related to changes in discounted life cycle costs associated with the aircraft. Predicted changes in aircraft price associated with changes in fuel cost were around 10% of the change in the discounted life cycle cost associated with the same fuel cost change. This seems reasonable, given that substantial portions of fuel price changes will be passed along to airline customers or result in changes in demand for seats as opposed to being absorbed by the aircraft manufacturers as price decreases. Also, only a portion of annual price changes will be interpreted by the market as affecting future prices.

The time trend parameters on *Year*$_{jt}$ indicated a decrease in real prices of 1.1% per year. Note that the GDP deflator was used to escalate nominal prices to constant 2016 dollars. For the recent period, this is consistent with a 1% annual rise in nominal prices.

Price Discounts From List Price and Boeing Financial Data

Estimates of transaction prices for commercial aircraft are often expressed as discounts from list prices. We calculated discounts from Boeing's 2016 list prices (which were unchanged from the published 2015 values) using both the MBA data and estimated prices from the models, including error bounds. An example using the pooled OLS MTOW model is shown in **Error! Reference source not found.**.

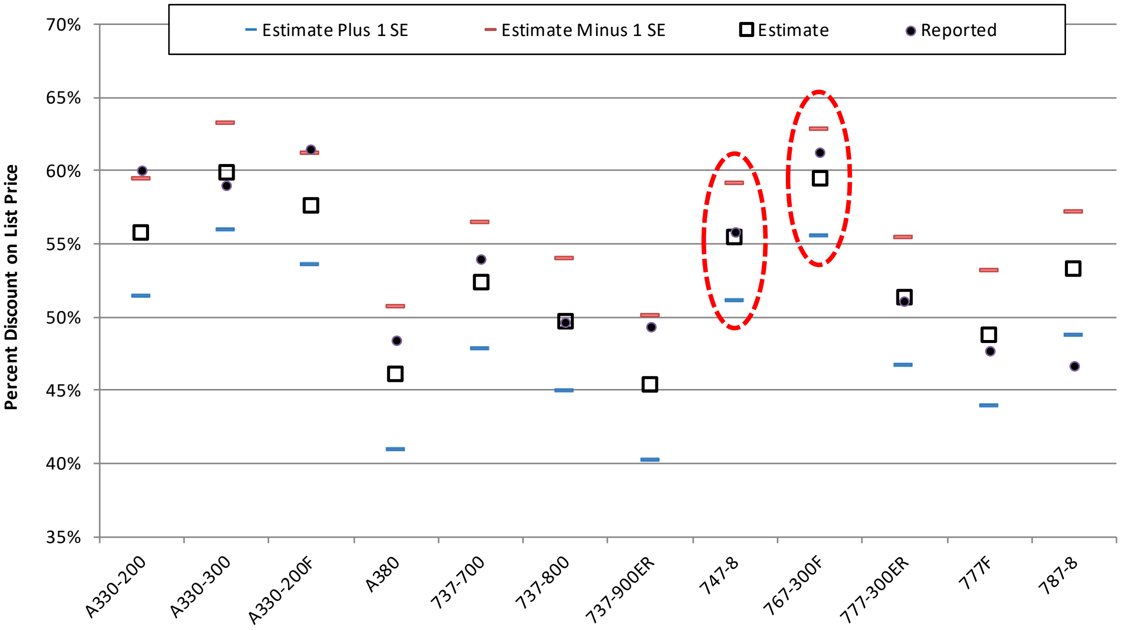


Figure 3. **Discounts From 2016 List Prices: MTOW Model**

For the WB aircraft, the average discount for Boeing aircraft was 53% for the MBA data and 52% for the MTOW model estimates. Over the entire Boeing portfolios, the average discount was 53% for the MBA data and 52% for the MTOW model estimates. For the Boeing portfolio, we also calculated weighted average discounts.

As a means of validating the models and the underlying MBA data, we calculated the weighted average discount for Boeing based on their reported financial data and aircraft deliveries for 2016. Boeing reported revenue by Segment including Commercial Airplanes (BCA), where revenue was booked at aircraft delivery. A small portion of BCA revenue is from commercial after-sales support (CAS) and was estimated to be $6.5 billion in 2014 (Broderick, 2014). Extrapolating this value forward using the annual growth rate from 2011 to 2014 of 6.4%, we arrived at a value of $7.355 billion for 2016.

We calculated aircraft sales revenues by subtracting CAS revenues from total BCA revenues for 2016:

$$R_t = \$65{,}069\text{M} - \$7{,}355\text{M} = \$57{,}714\text{M}.$$

Annual delivery quantities by model (q_{jt}) and list prices by model ($\overline{p}_{jt}^{*}$) are available for each model from Boeing's website. Given these values, the weighted average 2016 discount (D_t) was

$$D_t = \frac{R_t}{\sum_j \overline{p}_{jt}^{*} \mathrm{q}_{\mathrm{jt}}} - 1 = \frac{\$57{,}714M}{\$121{,}453M} - 1 = 52.5\%. \qquad (7)$$

Replacing $R_t$with the model estimates for each model $\hat{p}_{\mathrm{jt}}$ yielded the estimated weighted average discount ($\hat{D}_t$):

$$\hat{D}_t = \frac{\sum_j \hat{p}_{\mathrm{jt}} \mathrm{q}_{\mathrm{jt}}}{\sum_j \overline{p}_{jt}^{*} \mathrm{q}_{\mathrm{jt}}} - 1. \qquad (8)$$

$\hat{D}_t$ varied between 50.2% and 51.3%, depending upon which models were used to estimate $\hat{p}_{\mathrm{jt}}$. When the MBA values were used for $\hat{p}_{\mathrm{jt}}$, $\hat{D}_t$ = 50.1%. These results give some assurance, that at least at the top level, the MBA data and the models are consistent with Boeing's revenue derived from aircraft sales.

Another important result from the models was the estimated downward trend in real transaction prices over the sample period. Boeing applies a weighted average of input price inflation rates when escalating list prices from year to year. Given this, and the model results, we should expect calculated discounts from list prices to be increasing over time as list prices rise at a higher rate than transaction prices. This is what we see where D_t increased from 34–39% (depending on assumptions regarding CAS revenue) in 2004 to 52.5% for 2016 as calculated in Equation 7. These additional calculations using publicly available Boeing data also confirm modeling results and the underlying data used.

Example Application: KC-46A

In this chapter, we apply information from the economics literature, our modeling results, and other relevant data to help estimate "fair and reasonable" prices for the commercial aircraft platforms used for the KC-46A.

The KC-46A's commercial platform, the 767-2C, has features that have no direct analog in the commercial aircraft database. Boeing considers the platform to be based on the 767-200ER passenger aircraft, even though it has freighter floors and doors associated with the longer 767-300F. While the 767-300F is still in production, the last 767-200ER was delivered in 2008. The price estimating models do provide some flexibility in producing estimates of transaction prices. The model can take into account the implied value to the market of some characteristics of the 767-2C, such as the increased MTOW (415,000 lbs. versus 396,000 lbs. for the 767-200ER and 413,000 lbs. for the 767-300F).

The competitive nature of the initial down-select, including NTE prices for production lots through the end of the planned program, meant that the fair value of all 767-2C features was revealed and should guide future prices. In other situations, one approach to addressing the value of like-type features would be to add their cost basis along with a representative mark-up to price. The costs could be based on analogies, cost estimating relationships, or cost data from the seller. The government has the right to ask for seller cost data, although it need not be TINA-compliant.

However, the overall market conditions and the specifics of the 767 production that were obtained at the time of the 2011 competition (including expectations regarding the future) are likely to be different now. The MBA data, price estimating models, and Boeing financials show a continuing downward trend in real prices. Also, given additional 767-300F orders and deliveries for Federal Express, the overall 767 program is delivering aircraft at a rate higher than planned in 2011; given the relationship between cost and price for a mature program (where the z_t argument goes to 0 in the $p_t = \dfrac{c_t + z_t}{1-((1\text{-}s)/E)}$ equilibrium relation, and the denominator is less than 1), the delivery rates indicate a lower price, as fixed costs are allocated over more units in a given year.

We are able to capture the overall price trend by applying the pooled OLS model using 767-2C characteristics and time series inputs, including projections to 2020. Projections for GDP growth and fuel prices are taken from International Monetary Fund (IMF) forecasts (2016), while additional deliveries reflect Boeing planned 767 delivery rates of two aircraft/month (up from prior values of one aircraft/month). This is shown in **Error! Reference source not found.**, along with data and model results from the 767-200ER, model estimates of the 767-2C, as well as data for the 767-300F.

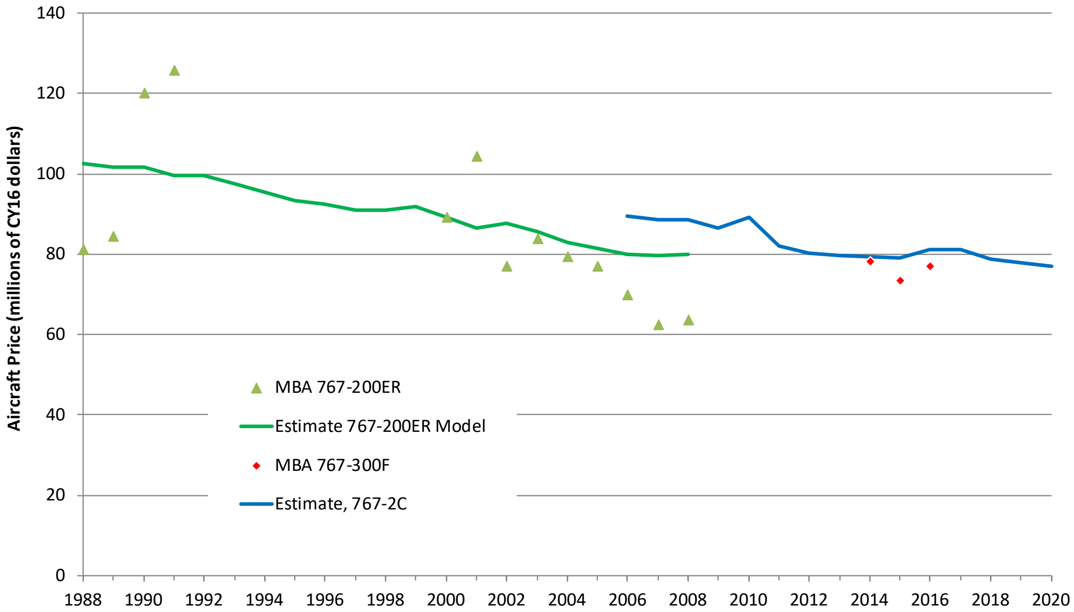


Figure 4. **Panel Data Model Estimates for the 767-2C With Comparisons**

The 2016 estimate for the 767-2C is $81.3 million in CY2016 dollars (note that this excludes KC-46A-specific provisions that are not captured in the model). Comparing this value to the model-predicted 2011 value shows an estimated decrease in price of 1.3%. In the case of 2017, the longer-term decrease in real prices is offset by price increases indicated by the model due to decreases in the fuel prices. This effect dissipates for future years with estimated prices decreasing to 6% below the 2011 value by 2020.[7] This indicates that there is room for negotiation below the NTE values determined in the 2011 competition. For later lots where the NTEs are subject to adjustment based on an EPA clause, if the price trends indicated by the data and model (including evidence from Boeing's financial data) diverge from the price index specified in the EPA clause, there is additional potential to negotiate prices below the NTEs (as adjusted by the EPA).

As mentioned in the description of the regression analyses, we cannot separate out the supply-side effects on price of increases in production rates from the demand-side effects (GDP growth in our preferred models) using the MBA data. However, given general knowledge of aircraft industry cost structures as well as specific information from Boeing's financial reporting, we can analytically derive an estimate of cost effects of the higher production rates. The cost/price effects of increased 767 production rates can then be approximated by employing a "rate slope" term as estimated in DoD programs where price is based on cost.[8] Information from Boeing financial statements regarding the cost of reducing 747 production rates provides a way to calibrate the rate slope model for commercial aircraft production. With this information, estimates of unit costs and fixed cost percentages at different delivery rates can be calculated. This is shown in **Error! Reference source not found.**, where delivery rates from 6/year to 18/year are included, consistent with 2015 experience and forecasts through 2021.

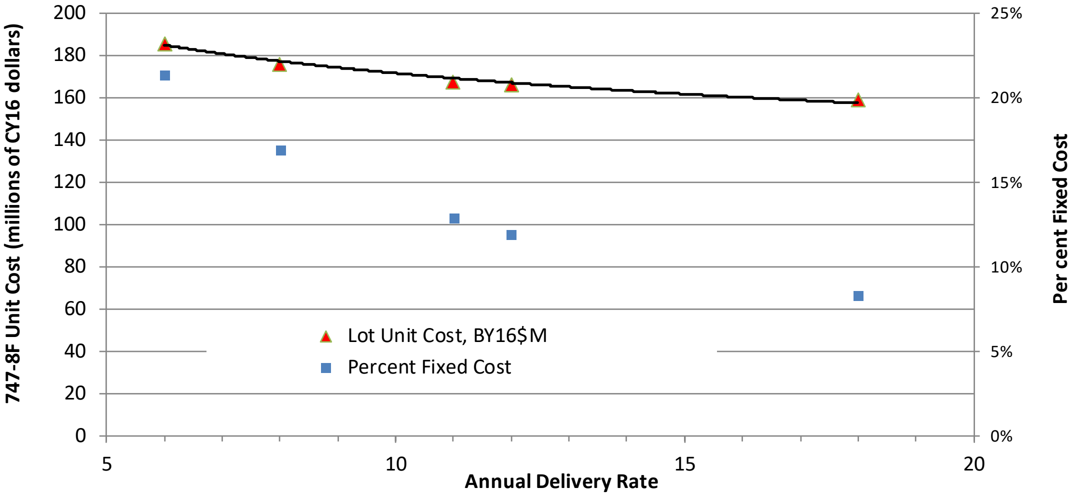


Figure 5. **Unit Cost and Fixed-Cost Percentage Estimates for 747 Production**

The curve fitted to the unit costs generalizes the relationship between annual quantities and unit costs; it is known as the "rate curve" relation,

$$c_t = \alpha \, \boldsymbol{q}_t{}^{\beta}, \qquad (9)$$

[7] This estimate is based on IMF forecasts of the price of Brent crude, which is projected to increase from an average of $43/barrel in 2016 to $54/barrel in 2019 (all nominal dollars).

[8] This approach was suggested by Dr. David Marzo of CAPE/CA.

where $\boldsymbol{q}_t$ is the annual delivery rate. For the 747 example above, the estimated □ coefficient is -.146, corresponding to a 90.4% rate slope; this is within the range of parameters estimated for military aircraft programs.

Taking model-estimated prices for the 767-2C and insights from the above 747 analyses, we can estimate cost decreases driven by increases in production rates between the plan at Boeing’s 2011 bid and the current plan. These differences indicate a 38% steady state increase in production rate. Baselining cost values to 767-2C price estimates for 2015 and applying the 15% margin assumption allows us to generate estimates of cost savings associated with the higher production rates. Using the 90.4% rate slope, we estimate annual unit cost savings of around $3 million (CY16) for the steady state years (2017 to 2026), corresponding to a 2% decrease in cost.

The 767-2C presents a special case, as price discovery at the time of competition between alternative tankers means that there is less uncertainty for future purchases. However, we see in the application of our models and other information that there are both program-specific factors (higher than previously planned production rates) and overall industry trends (increases in nominal prices over time that are less than overall inflation) that would indicate prices below the NTEs could be negotiated for future lots.

The long time horizon for the KC-46A program means that it is important to take into account both the effect of general industry pricing trends and changes in the specifics of 767 production economics. Our analyses of both of these effects indicate that the government may be able to pay lower prices than the NTE prices set in the original competition.

Commercial Aircraft Pricing Lessons Learned

Commercial Aircraft Pricing Tools

Price determination by negotiation for commercial items will generally only occur if the supporting markets are not purely competitive. In the case of commercial aircraft, the market is a duopoly where prices are above those that would be paid if the market were purely competitive. The specifics of this market have been explored in some detail in the economics literature. The resulting game-theory models are insightful but without much empirical gain. We were able to make use of the consultant-reported transaction prices to quantify price drivers, both on the demand and supply side of the market, through least-squares regression analyses. These models explain most of the variance in prices across aircraft models and time; utility associated with commercial airline services, moving people and goods speedily across long distances, can be proxied effectively by a small number of variables, while supply/cost effects can be mostly captured in a few dimensions. An important insight from the models and supporting data is the long-run decrease in real commercial aircraft prices. This could have an important impact on the pricing of future KC-46A procurements.

The models are useful in establishing baseline values for commercial aircraft used by the military. In our application of the models to the KC-46A program, we needed additional tools and data to address specifics of that program/aircraft. This included cost drivers not captured in the models (production rate effects).

Implications for Other Commercial Items

Several steps in the analysis of the commercial aircraft pricing for military applications would be relevant in negotiating prices for other commercial items:

- Understand the market in which the seller operates. This would go beyond "market research" and should address market dynamics as described by economic theory.
- Model market prices as they relate to both supply-side (cost) and demand-side (utility) drivers. This will be challenging in that most commercial items bought by the DoD and subject to price negotiation will not be as homogenous as commercial aircraft.
- Make use of the seller's publicly available financial data to put available pricing data into perspective—and to better understand the seller's business model.
- Given the existence of "like-type" modifications to items available on the commercial market, it may be advantageous to estimate the discrete costs of these modifications.

References

Airline Monitor. (n.d.). Retrieved from http://airlinemonitor.com/

AVITAS. (n.d.). *Bluebooks*. Retrieved from https://www.avitas.com/

Baldwin, R., & Krugman, P. (1988). Industrial policy and international competition in wide-bodied jet aircraft. In R. Baldwin (Ed.), *Trade policy issues and empirical analysis* (pp. 45–78). Chicago, IL: University of Chicago Press for the National Bureau of Economic Research.

Bechai, D. (2016). Does a $7 million Boeing 777-200ER compare to a brand new dreamliner? (Part 1). Retrieved from https://seekingalpha.com/article/3956517-7-million-boeing-777minus-200er-compare-brand-new-dreamliner-part-1

Benkard, C. L. (2004). A dynamic analysis of the market for wide-bodied commercial aircraft. *Review of Economic Studies, 71*(3), 581–611. doi:10.1111/j.1467-937X.2004.00297.x

Broderick, S. (2014). Boeing revives emphasis on post-delivery business. Retrieved from http://aviationweek.com/mro/boeing-revives-emphasis-post-delivery-business

DoD. (2016). *Selected acquisition report (SAR), KC-46A tanker modernization (KC-46A) as of FY 2017*. Washington, DC: Author.

DoD Defense Standardization Program. (n.d.). Key policy documents. Retrieved from http://www.dsp.dla.mil/Policy-Guidance/Key-Policy-Documents/

Greene, W. H. (2002). *Econometric analysis* (5th ed.). Upper Saddle River, NJ: Prentice Hall.

Harmon, B. R., Sullivan, C. D., & Davis, G. A. (2010). *Pricing of commercial airliners and engines* (IDA Paper P-4683). Alexandria, VA: Institute for Defense Analyses.

Hodrick, R. J., & Prescott, E. C. (1997). Postwar U.S. business cycles: An empirical investigation. *Journal of Money, Credit and Banking, 29*(1), 1–16. Retrieved from http://www.jstor.org/stable/2953682

International Monetary Fund. (2016). World economic outlook, subdued demand: Symptoms and remedies. Retrieved from http://www.imf.org/en/Publications/WEO/Issues/2016/12/31/Subdued-Demand-Symptoms-and-Remedies

Irwin, D. A., & Pavcnik, N. (2004). Airbus versus Boeing revisited: International competition in the aircraft market. *Journal of International Economics, 64*(2), 223–245. doi:10.1016/j.jinteco.2003.08.006

Kronemer, A., & Henneberger. J. E. (1993). Productivity in aircraft manufacturing. *Monthly Labor Review,* 24–33. Retrieved from https://www.bls.gov/mfp/mprkh93.pdf

Markish, J. (2002). *Valuation techniques for commercial aircraft program design* (Master's thesis). Retrieved from http://hdl.handle.net/1721.1/16871

Morten Beyer & Agnew (MBA). (n.d.). Retrieved from https://www.mba.aero

Nelson, J. R., Woolsey, J. P., Harmon, B. R., Arnold, S. A., & Park, B. K. (2003). *Purchase price estimate for the KC-767A tanker aircraft (redacted version)* (IDA Paper P-3802). Alexandria, VA: Institute for Defense Analyses. (Unclassified//FOUO)

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. (n.d.). *Commercial item handbook (version 2.0)*. Washington, DC: Author.

U.S. Energy Information Administration. (n.d.). U.S. kerosene-type jet fuel retail sales by refiners. Retrieved from https://www.eia.gov/dnav/pet/hist/LeafHandler.ashx?n=PET&s=EMA_EPJK_PTG_NUS_DPG&f=M

Towards the Dynamic Contracting of Verification Activities With Set-Based Design: An Initial Model of Rework

Peng Xu—is a PhD student with the Grado Department of Industrial and Systems Engineering at Virginia Tech. He received his MS in mechanical engineering from National Cheng Kung University in 2015 and his BS in mechanical engineering from Shandong University in 2013. His research interests include complex system diagnosis, dynamic decision making, and knowledge elicitation. [xupeng@vt.edu]

Alejandro Salado—is an Assistant Professor with the Grado Department of Industrial and Systems Engineering at Virginia Tech. His research focuses on applying decision analysis to improve the practice of engineering, in particular in the areas of verification and validation, and on improving problem formulation through modeling. Dr. Salado is a recipient of the NSF CAREER Award and the Fulbright International Science and Technology Award. He holds a BSc and an MSc in electrical engineering (Polytechnic University of Valencia), an MSc in project management and an MSc in electronics engineering (Polytechnic University of Catalonia), the SpaceTech MEng in space systems engineering (Delft University of Technology), and a PhD in systems engineering (Stevens Institute of Technology). [asalado@vt.edu]

Abstract

This paper is intended to disseminate initial outcomes of the NPS Research Acquisition Program "Dynamic Contracting of Verification Activities by Applying Set-Based Design to the Definition of Verification Strategies" project. Verification activities provide the evidence of contractual fulfillment. In current practice, a verification strategy is defined at the beginning of an acquisition program and is agreed upon by customer and contractor at contract signature. This research project shows that contractually committing to a fixed verification strategy at the beginning of an acquisition program fundamentally leads to suboptimal acquisition performance. This is caused by the uncertain nature of system development, which will make, as it progresses, verification activities that were not previously planned necessary and will make some of the planned ones unnecessary. Therefore, dynamic contracting of verification activities is necessary to guarantee optimality of acquisition programs in this area. Such an approach to contracting may be enabled by applying set-based design to the definition of verification strategies. This paper provides a summary of such an approach and contributes with a refined model of rework activities that may be undertaken to increase the confidence on the proper functioning of the system as verification results become known.

Introduction

Verification activities, which usually take the form of a combination of analyses, inspections, and tests, consume a significant part, if not the biggest part, of the development costs of large-scale engineered systems (Engel, 2010). Verification occurs at various integration levels and at different times during its life cycle (Engel, 2010). Under a common master plan, low level verification activities are executed as risk mitigation activities, such as early identification of problems, or because some of them are not possible at higher levels of integration (Engel, 2010). Therefore, a verification strategy is defined as

> aiming at maximizing confidence on verification coverage, which facilitates convincing a customer that contractual obligations have been met; minimizing risk of undetected problems, which is important for a manufacturer's reputation and to ensure customer satisfaction once the

> system is operational; and minimizing invested effort, which is related to manufacturer's profit. (Salado, 2015)

Essentially, verification activities are the vehicle by which contractors can collect evidence of contractual fulfillment in acquisition programs.

In current practice, a verification strategy is defined at the beginning of an acquisition program and is agreed upon by the customer and contractor at contract signature. Hence, the resources necessary to execute verification activities at various stages of the system development are allocated and committed at the beginning, when a small amount of knowledge about the system is available (Engel, 2010). However, the necessity and value of a verification activity cannot be measured independently of the overall verification strategy (Salado & Kannan, 2018b). Instead, the necessity to perform a given verification activity depends on the results of all verification activities that have been previously performed (Salado & Kannan, 2018b). For example, testing the mass of a component is considered more necessary if a previous analysis has shown low margin with respect to the success criterion than if the analysis has shown ample margin. Thus, contractually committing to a fixed verification strategy at the beginning of an acquisition program fundamentally leads to suboptimal acquisition performance. Essentially, the uncertain nature of system development will make verification activities that were not previously planned necessary and will make some of the planned ones unnecessary (Salado & Kannan, 2018b). The former can be handled through change requests (CRs), but they require unplanned financial investments. The latter can be recovered in a few cases through negative change requests, but, in general, they imply a waste of the financial investment because the investment has been committed to the contractor.

In this context, dynamic contracting of verification activities becomes necessary to guarantee optimality of acquisition programs in this area (Xu & Salado, 2019). Instead of contracting a predefined set of activities at the beginning of a project, the necessity and contracting of each verification activity (or subsets of them) are evaluated and executed as the system development progresses (Xu & Salado, 2019). Set-based design has been proposed as part of this research to support such a contracting approach (Xu & Salado, 2019). Informed by the benefits of set-based design in conceptual design (Singer, Doerry, & Buckley, 2009), an overall set of verification activities is considered, but not contracted, at the beginning of a project. A vector of investment opportunities indicates the development stages in which verification activities may be contracted and executed. Based on their results, the set of remaining verification paths to the end of the system development is updated (Xu & Salado, 2019).

This paper presents the current state of the research project and contributes with a refined model of rework activities that may be undertaken to increase the confidence on the proper functioning of the system as verification results become known.

Background: Models of Verification Strategies

Primary Characteristics of Verification As An Engineering Endeavor

Consider

a generic model of the expected utility $E\left[U_{S,p,t}\right]$ provided by a system S at time t with respect to a set of preferences P, as given in Eq. (1),

$$E\left[U_{S,P,t}\right]=F_U\left(S_A,B_t\left(S_A,t_n\right),P\right) \tag{1}$$

> where S_A is a set of system characteristics, $B_t\left(S_A, t_n\right)$ is the belief at time t that those system characteristics will be exhibited by the system at a later time t_n, and F_U is a set of expected utility functions, associated with beliefs on those functions, that map system attributes, beliefs of system attributes, and preferences to expected utility. (Salado & Kannan, 2018b)

In this context, a verification activity is one that "affects at least $B_t\left(S_A, t_n\right)$" (Salado & Kannan, 2018b). That is, a verification activity is one that, as a minimum, provides information about the system under development.

For the purpose of this paper, two main characteristics of verification lead to the need for dynamic contracting of verification strategies. First, the value of each verification activity is not absolute, but depends on the results of prior verification activities (Salado & Kannan, 2018b). As explained in the introduction of this paper, this means that the value of a verification activity cannot be determined individually, but in the context of the knowledge at the time of executing the activity. Therefore, the expected value provided by a verification activity evolves as a function of the results of previous verification activities. Second, although verification activities are objective, the confidence that they generate is subjective (Salado & Kannan, 2018b). This means that not only prior verification activities influence the value of a verification activity, but also the engineer or the team in charge of processing and interpreting the results of a given verification activity do so. Given the long development times necessary in some large-scale systems, it is common that the team in charge of executing verification activities towards the later stages of the system development is different from the team that planned those verification activities early in the lifecycle. Hence, changes in the perceived value of a verification activity are inherent to the nature of a large-scale system development, under the assumption that the teams will change as the development progresses.

Mathematical Models of Verification Strategies

In this paper, a verification strategy is understood to be a set of verification activities organized as an acyclic directed graph (Salado & Kannan, 2018a). A verification activity is understood to be the collection of information about a specific aspect of the system under development (for simplicity we will call this a system parameter) and verification evidence refers to such information. Furthermore, it is assumed that the level of confidence in the correct performance of the system is shaped by the system architecture (e.g., maturity and coupling of the system's components) and the results of the various verification activities (Salado & Kannan, 2019).

Mathematically, this understanding is captured by "modeling the engineer's posterior belief distribution $\pi(\theta \mid \mathbf{s})$ based on his/her prior belief distribution $\pi(\theta)$ and the density function $f(\mathbf{v} \mid \theta)$, conditioned on the collected verification evidence $\mathbf{v}$", where θ is the system parameter that is verified and $\mathbf{v} \in V^*$ is a specific vector of verification results (or verification evidence) (Salado & Kannan, 2019). Using this mathematical framework, a verification strategy is modeled as a Bayesian network $BN = \Upsilon \cup A \cup B$, where (Salado & Kannan, 2019):

- $\Upsilon = (V, D)$ is a simple directed graph that captures the planned execution of verification activities. The set V is a set of verification activities, and D is a set of tuples (a, b), with $a, b \in V$, that describes the relative order in which verification activities are planned to be executed (Salado & Kannan, 2018a).

- $A=\left(\theta_Z, D_\theta\right)$ is a simple directed graph that captures the properties of the system architecture, specifically the coupling between the different components forming the system, as well as their individual maturity. The set θ_Z captures the prior beliefs on the absence of errors in the system parameters, and the information dependencies between those parameters are captured in the set $D_\theta=\left\{(a,b): a,b \in \theta_Z, f\left(b \mid \mathbf{a}\right) \neq f\left(b\right)\right\}$.

  $B=\left(\left\{\theta_Z, V\right\}, D_\Upsilon\right)$ is a simple directed graph that captures the ability of the verification activities to provide information about one or more system parameters, where $D_\Upsilon=\left\{(a,b): a \in \theta_Z, b \in V, f\left(b \mid \mathbf{a}\right) \neq f\left(b\right)\right\}$.

Resulting graphs modeling verification strategies can be reduced to a combination of a finite set of patterns (Salado & Kannan, 2019). Identification of patterns may aid in interpreting the role of the various verification activities within a strategy. For example, a dynamic network (as will be used later in this paper) indicates that certain activities may make some prior activities irrelevant once the new ones have been executed (Salado & Kannan, 2019).

It should be noted that the previous notation may not be followed throughout the paper; it has been used here for consistency with the original source.

A Concept for Dynamic Contracting of Verification Activities

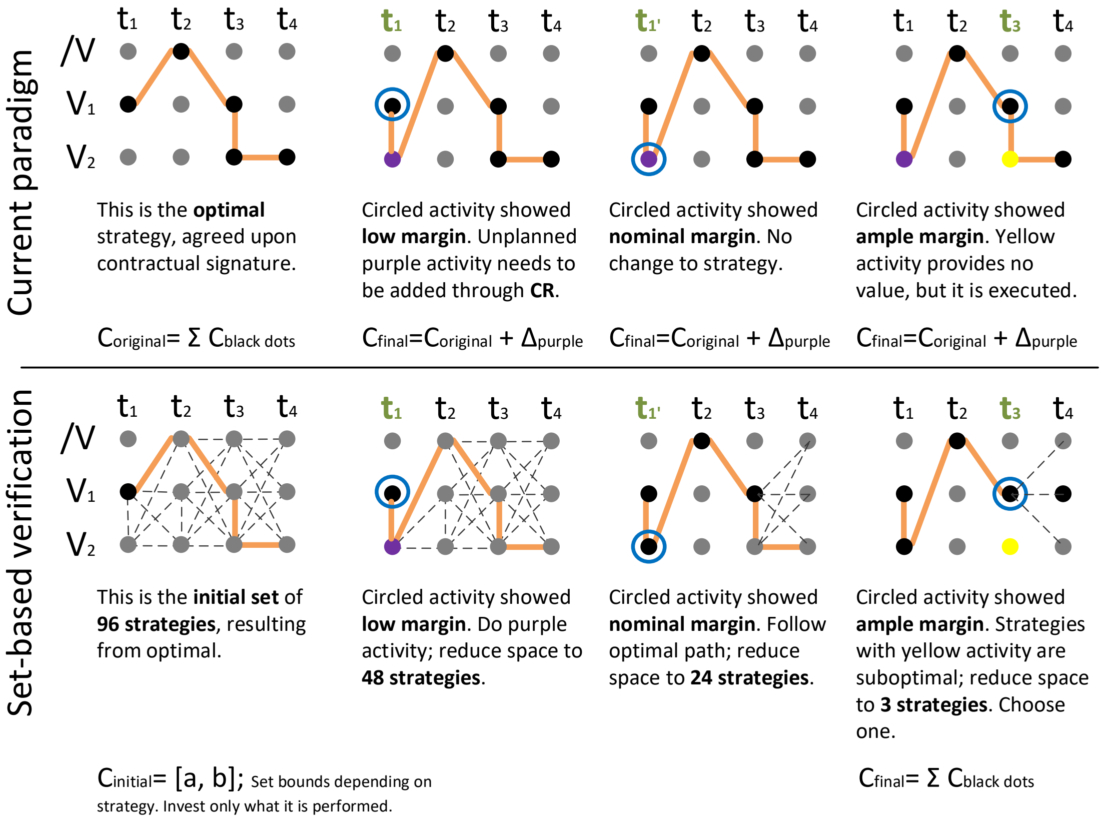
The concept for dynamic contracting of verification activities has been presented in Xu and Salado (2019) and is depicted in Figure 1 in comparison with the current approach. The following description is reproduced verbatim from the original source:

> In the current paradigm (top part of the figure), a contract for a verification strategy is fixed at the beginning of the system development program. The strategy is defined by the black dots connected by the orange line, which represent the verification activities that will be executed throughout the system development.
>
> Without loss of generality, it is possible to assume that such verification strategy was determined optimal at the beginning of the program, that is, with the knowledge available at that point in time. Consider now that the verification activity V_1 at t_1 shows a tight margin with respect to the expected result of the activity. This may lead to a lower than expected confidence on the system being absent of errors that triggers the need for an additional, unplanned verification activity V_2 at t_1. Because the contract was fixed, such an activity needs to be contractually introduced through a change request.
>
> Consider on the contrary, that the verification activity V_1 at t_3 showed much better results than previously expected. This may yield a higher than expected confidence on the system being absent of errors, potentially making verification activity V_2 at t_3 unnecessary or of little value, because of how confidence builds up on prior information (Salado & Kannan, 2018b; Salado, Kannan, & Farkhondehmaal, 2018).

Consider now the proposed set-based design approach, depicted on the bottom side of Figure 2. In this case, an optimal strategy is also determined at t_1. However, because the value of verification activities may change as results become available (Salado & Kannan, 2018b), a set (represented by the dotted lines connecting the dots) is considered instead of just one strategy, and only the first verification activity V_1 at t_1 is contracted at this point. This set is the set of all possible verification strategies that are consistent with the optimal verification strategy (that is, formed by all verification strategies that have the first activity in common).

Assume then that verification activity V_1 at t_1 provides low margin with respect to the expected results, as was the case before. With the updated confidence level, a new optimal strategy is selected within the remaining set. Then, the set is reduced to include only those verification activities that are consistent with the new optimal strategy. In this way, verification activity V_2 at t_1 is contracted as well. The process of identifying new optimal strategies based on updated confidence and reducing the set of remaining verification activities to those consistent with the new optimal strategy, continues at each t.

Assume later in the system development that, as was the case when describing the current paradigm, verification activity V_1 at t_3 shows ample margin with respect to the expected result. The next assessment of the remaining optimal path yields a set of verification strategies that do not include verification activity V_2 at t_3. Based on this result, V_2 is not contracted at t_3. Consequently, this approach does not waste resources in activities that become no longer needed as verification evidence becomes available. (Xu & Salado, 2019)



This is the **optimal** strategy, agreed upon contractual signature.

Circled activity showed **low margin**. Unplanned purple activity needs to be added through **CR**.

Circled activity showed **nominal margin**. No change to strategy.

Circled activity showed **ample margin**. Yellow activity provides no value, but it is executed.

$C_{original} = \Sigma\, C_{black\ dots}$ $C_{final} = C_{original} + \Delta_{purple}$ $C_{final} = C_{original} + \Delta_{purple}$ $C_{final} = C_{original} + \Delta_{purple}$

This is the **initial set** of **96 strategies**, resulting from optimal.

Circled activity showed **low margin**. Do purple activity; reduce space to **48 strategies**.

Circled activity showed **nominal margin**. Follow optimal path; reduce space to **24 strategies**.

Circled activity showed **ample margin**. Strategies with yellow activity are suboptimal; reduce space to **3 strategies**. Choose one.

$C_{initial} = [a, b]$; Set bounds depending on strategy. Invest only what it is performed.

$C_{final} = \Sigma\, C_{black\ dots}$

Figure 1. **Current vs. Set-Based Approaches for Designing Verification Strategies**

(Xu & Salado, 2019)

Note. C: cost of executing verification; t_i: verification events; /V: no verification; V_i: verification activity.

Applying Set-Based Design to the Design of Verification Strategies

The lack of knowledge in early design activities motivated the emergence of set-based design (Bernstein, 1998). Set-based design is built on the principle of working simultaneously with a plethora of design alternatives, instead of converging quickly to a single option (Bernstein, 1998). As the knowledge about the system increases, suboptimal alternatives are discarded until a preferred one remains (Bernstein, 1998). A key aspect is that discarding is not an activity at a given point of time, like a traditional trade-off, but a time-continuous activity that occurs as new knowledge is available (Bernstein, 1998). A formal formulation of set-based design and how it makes product development resilient against changes in external factors is given in Rapp et al. (2018). The approach has been successfully applied in the conceptual stages of naval systems (Singer, Doerry, & Buckley, 2009), graphic industry products (Raudberget, 2010), automotive products (Raudberget, 2010), and aeronautic systems (Bernstein, 1998), among others.

As discussed in the introduction, these findings informed the application of set-based design to the design of verification strategies (Xu & Salado, 2019). The benefits of set-based design were explored in a notional case study with synthetic data. Results indicated that set-based approach yielded higher expected value. In addition, set-based design seemed to respond faster to adjusting its parameters than the benchmark when receiving information from verification evidence, which indicates “the benchmark approach is inefficient when compared against the proposed set-based approach” (Xu & Salado, 2019). Further research is necessary to confirm these findings, though.

The basic process proposed to apply set-based design to the design of verification strategies consists of the following steps (Xu & Salado, 2019):

Step 1. Determine optimal verification strategy at Time 1.

Step 2. Choose first (timewise) verification activity (or subset of verification activities).

Step 3. Execute activity and update Bayesian network.

Step 4. Determine optimal remaining verification strategy and return to Step 2.

After each selection of an optimal strategy, the set of potential verification strategies is given by those strategies that share the first (timewise) verification activity (or subset of verification activities). Therefore, as the optimal remaining verification strategies are determined, the set shrinks until verification is completed.

In addition, the set of verification strategies can be further reduced by eliminating those sets that are dominated by optimal strategies throughout the system development. This reduction is useful for managing the resulting complexity. An example of the evolution of the set of verification strategies after applying set-based design is provided in (Xu & Salado, 2019) and shown in Figure 2. At T_1, the optimal verification strategy contains V_1 at T_1. Two results are considered; either the activity *passes* or *fails*. In each case, the optimal strategy out of the set of remaining strategies can be computed. In both cases, the optimal strategy contains V_2 at T_2. The process continues by assessing how the optimal strategy changes on each path as the results of the next verification activity (in this case V_2 in each path) are known. This process is repeated until T_5. It should be noted how the result of each verification activity changes the optimality of the remaining verification strategy.

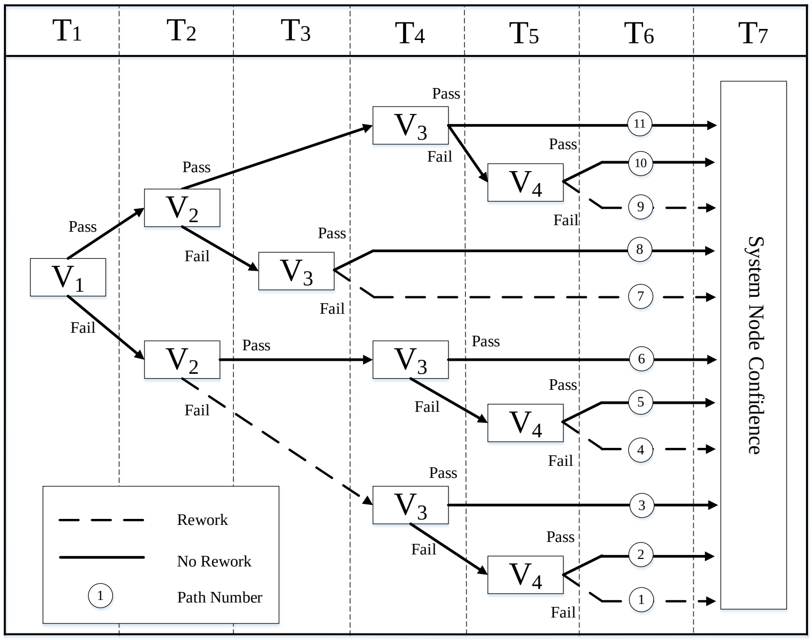


Figure 2. **Verification Path Tree**
(Xu & Salado, 2019)

Overall in this example, 11 verification strategies dominate every other verification strategy in the set. Because of this, it suffices to work with an initial set of verification strategies (i.e., before T_1) that contains those eleven strategies. In case V_1 passes, the set shrinks to contain five strategies (strategies 7 to 11) after T_1 and before T_2. Otherwise, the set shrinks to contain six strategies (strategies 1 to 6). This process continuous until verification is completed. This evolution is consistent with the set-based design paradigm, since multiple alternatives are considered simultaneously and some of them are progressively discarded from the set until a single alternative finally remains.

A Refined Model of Rework

Background

In prior work, rework has been treated as a predefined decision based on the achieved confidence (Xu & Salado, 2019). Specifically, if the confidence in the correct functioning of the system (for example, as represented by parameter θ in the section entitled Mathematical Models of Verification Strategies) would fall below a certain threshold, then a rework activity was considered to be executed automatically. In this paper, we present a model of rework activities that considers a different decision mechanism. In particular, a rework activity is initiated if a verification activity fails.

Problem Statement

Consider the simple overarching verification network in Figure 3. It represents the way in which a set of available verification activities provide information about a system parameter θ_S (e.g., the mass of the system). In the figure, θ_C represents another parameter that provides information about θ_S (e.g., the mass of a system component), V_1 is a verification activity that provides information about θ_C (e.g., a test of the mass of a system component), and V_2 is a verification activity that provides information about θ_S (e.g., a test of the mass of the system).

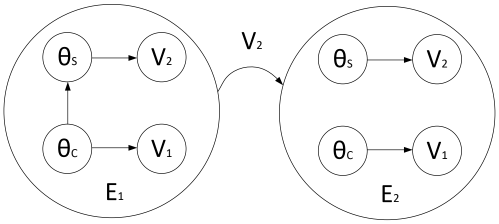


Figure 3. **Overarching Verification Network**

Five verification strategies can be devised by leveraging the overarching network (notation from Salado and Kannan, 2018a, is used):

$$S_1 = (\varnothing, \varnothing)$$

$$S_2 = (\{V_1\}, \varnothing)$$

$$S_3 = (\{V_2\}, \varnothing)$$

$$S_4 = (\{V_1, V_2\}, \{(V_1, V_2)\})$$

$$S_5 = (\{V_1, V_2\}, \{(V_2, V_1)\})$$

It is assumed that S_5 is not meaningful, and therefore it will not be further considered.

The cost to execute a verification activity is denoted by σ_V. Table 1 lists the cost to execute each verification strategy. It is assumed that no overlap exists in the cost of executing the verification activities.

Table 1. Cost to Execute Verification Strategies

Strategy	Cost function
S_1	$\sigma_V(S_1) = \$0$
S_2	$\sigma_V(S_2) = \sigma_V(V_1) = \$200\text{K}$
S_3	$\sigma_V(S_3) = \sigma_V(V_2) = \$200\text{K}$
S_4	$\sigma_V(S_4) = \sigma_V(V_1) + \sigma_V(V_2)$

The cost impact associated to deploying the system with an error is denoted by σ_I. Table 2 lists the expected costs of impact for each strategy. It is assumed that $\sigma_I = 10{,}000\text{K}$.

Table 2. Impact Cost of Deploying the System With an Error

Strategy	Cost function
S_1	$E\left[\sigma_I(S_1)\right] = P(\theta_S = e)\cdot\sigma_I$
S_2	$E\left[\sigma_I(S_2)\right] = P(\theta_S = e \mid V_1 = p)\cdot\sigma_I$
S_3	$E\left[\sigma_I(S_3)\right] = P(\theta_S = e \mid V_2 = p)\cdot\sigma_I$
S_4	$E\left[\sigma_I(S_4)\right] = P(\theta_S = e \mid V_1 = p, V_2 = p)\cdot\sigma_I$

Note that $E\left[\sigma_I(S_3)\right] = E\left[\sigma_I(S_4)\right]$ because V_1 becomes disconnected from θ_S once V_2 is known.

Model of Rework Cost

Rework cost is denoted by σ_R. The key aspect is that the cost of rework will depend on when the rework happens or, more accurately, on whether rework requires integration and de-integration activities or not. Hence, it is necessary to capture the cause of the error, as well as the moment in which the error is found. It is assumed that rework results in a state of knowledge equivalent to $V = p$. This is because in the theoretical framework used in this paper, system attributes are not accessible; the only verification evidence is Salado and Kannan (2019).

Contrary to previous work, it is assumed in this paper that rework is performed as soon as a verification activity fails. This implies the following:

- For S_1, $E\left[\sigma_R(S_1)\right] = 0$ because, since there is no verification activity executed, errors cannot be found and rework activities initiated.

- For S_2, $E\left[\sigma_R\left(S_2\right)\right] = P\left(V_1 = \neg p\right) \cdot \sigma_R\left(C, C\right)$, where $\sigma_R\left(A, B\right)$ indicates that rework happens for assembly *A* when integrated at assembly level *B*. In this case, $\left(C, C\right)$ means that rework happens on the component when it is at the component level (that is, when the component is not integrated at system level). Only $\sigma_R\left(C, C\right)$ is considered in the model because, since no verification at system level occurs, errors can only be found at the component level.

Calculation for S_3 becomes more sophisticated because while the failure is detected on a verification activity at the system level, the error may result from an error at system level and/or an error at component level (note that in some cases solving the problem at the component level automatically solves the problem at the system level, and in some cases the system level problem persists and also needs to be fixed). This needs to be considered in the calculation of the expected rework cost. The following basic algorithm is used:

1. If an error is found, try to solve at system level.
2. If not solvable, try also at component level.

Note that a different algorithm could have been defined, trying to fix the problem at component level before trying at the system level. However, based on experience, it has been assumed that de-integration activities are less preferred. Under these conditions, the expected rework cost for S_3 is given by Equation 2:

$$E\left[\sigma_R\left(S_3\right)\right] = P\left(V_2 = f\right) \cdot \left[\sigma_R\left(S, S\right) + P\left(\theta_S = e, \theta_C = e \,|\, V_2 = f\right) \cdot \sigma_R\left(C, S\right)\right]. \qquad (2)$$

The following aspect is of interest in the previous equation. Note that, if the verification activity fails, rework automatically happens at the system level. As stated, rework at the component level is performed only if the problem persists. This is modeled by the probability that there is an error at both the system level and the component level. This is because

1. If the error was only at the system level, then the rework at system level would fix it.
2. If the error was only at the component level, then there is not really a problem at system level and the fix would also work.
3. The cost of rework at the system level is already accounted for, so this is why only the cost of the component level fixed is considered in that case.

Calculation for S_4 builds upon the same idea:

1. If the component level verification activity fails, then a rework activity at the component level occurs. Afterwards, if the system level verification activity fails, the same situation as in S_2 applies, with the difference that probability of errors is conditioned to the component level activity passed (because of the rework activity).
2. If the component level verification activity passes and then the system level verification activity fails, the same situation as in S_3 applies, with the difference that probability of errors is conditioned to the component level activity passed.

Under these conditions, the expected rework cost for S_4 is given by Equation 3:

$$E\left[\sigma_R\left(S_4\right)\right]=P\left(V_1=f\right)\cdot\left(\sigma_R\left(C,C\right)+P\left(V_2=f\,|\,V_1=p\right)\cdot\sigma_R\left(S,S\right)\right)+P\left(V_1=p\right)\cdot P\left(V_2=f\,|\,V_1=p\right)\cdot \left(\sigma_R\left(S,S\right)+P\left(\theta_S=e,\theta_C=e\,|\,V_2=f,V_1=p\right)\cdot\sigma_R\left(C,S\right)\right) \tag{3}$$

Table 3 lists the corresponding rework cost used in the model.

Table 3. Rework Costs

$\sigma_R\left(x,y\right)$		y	
		C	**S**
x	**C**	$200K	$1,000K
	S	n/a	$500K

Input Data

Cost figures are synthetic and given in the previous section, Model of Rework Cost. Probability assignments use synthetic data and are given in Tables 4 through 7. Following the modeling approach presented in Salado and Kannan (2019), prior beliefs are assigned to system parameter nodes, which capture the initial belief on the state of the system (i.e., being absent of errors), and conditional probability tables are created for the verification activity nodes. Posterior beliefs are calculated for system parameters through Bayesian update of the outcomes of the verification activity nodes. Probability update was conducted in this study using the Bayesian Network Toolbox for MATLAB®, which estimates the posterior probabilities of all nodes by the variable elimination method.

Table 4. Conditional Probability Table for System Parameter

θ_C	θ_S	$P\left(\theta_S\,|\,\theta_C\right)$
Error	Error	0.79
Error	No Error	0.21
No Error	Error	0.27
No Error	No Error	0.73

Table 5. Prior Probabilities of the Component Parameter

θ_C	$P\left(\theta_C\right)$
Error	0.20
No Error	0.80

Table 6. Conditional Probability Table for Verification Activity V_1

θ_C	V_1	$P(V_1 \mid \theta_C)$
Error	Fail	0.73
Error	Pass	0.27
No Error	Fail	0.05
No Error	Pass	0.95

Table 7. Conditional Probability Table for Verification Activity V_2

θ_S	V_2	$P(V_2 \mid \theta_S)$
Error	Fail	0.85
Error	Pass	0.15
No Error	Fail	0.18
No Error	Pass	0.82

Results and Discussion

Because of the size of the network and the input data, this case is not able to distinguish between the current acquisition paradigm and set-based design. However, the case is only used to explore the application of the refined rework model, so the case is still useful.

Results are shown in Figure 4. Two time events are represented, one at Time Interval = 1 (denoted by T_1) and one at Time Interval = 2 (denoted by T_2). Verification activities V_1 and V_2 are conducted at T_1 and T_2, respectively. Solid continuous lines are used for visualization purposes. Bifurcations differentiate the cost of potential paths should the verification activity pass or fail. Because of the set up of the case, the cost differences are caused only by the rework actions. The paths with positive slope indicate that the verification activity failed and, consequently, a rework activity was initiated. On the contrary, the paths with negative slope indicate that the verification activity passed and, consequently, rework activity was not initiated. The key insight of the picture is the consistency with which rework at different levels of integration is treated, in line with the input data. As can be seen, the delta rework cost after V_2 is larger than after V_1. This is, as discussed, because not only is rework at higher integration levels more expensive, but also, there is a chance that the problem at system level is caused by a problem at component level. Such de-integration effort considerably increases the resulting rework cost.

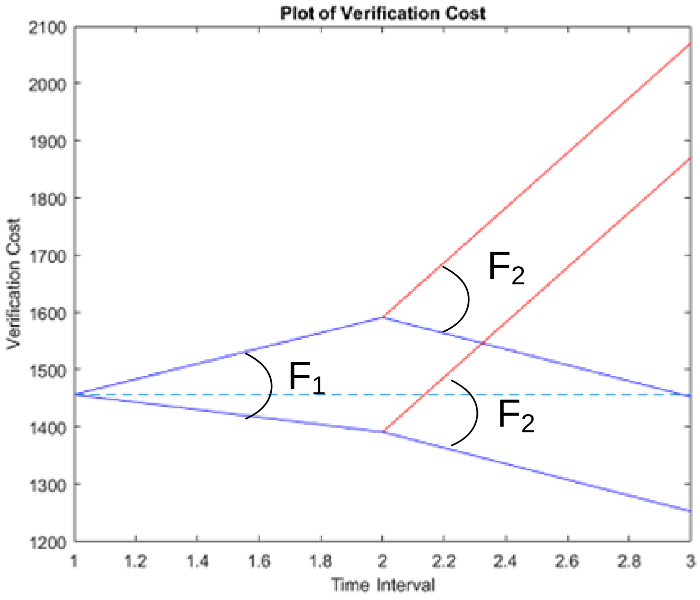


Figure 4. **Plot of Verification Paths**

Conclusions

This paper has shown that current approaches to contracting verification strategies in acquisition programs conflict with the inherent nature of verification. As a result, verification strategies in acquisition programs are set to suboptimality. This paper supports the idea of using dynamic contracting to overcome this problem. In this proposed approach, contracting of verification activities is spread throughout the system development. Instead of pre-agreeing on a fixed set of activities, verification activities are contracted at different points during the development. In this way, the results of prior verification activities can be used to determine the optimal path going forward in the system development.

Set-based design, which has been successfully applied in conceptual design and system architecture, provides a conceptual framework that can enable the dynamic contracting of verification strategies. Exploratory prior work seems to indicate that the set-based approach is stronger than the current paradigms for contracting of verification to deal with the uncertain nature of system development, yielding strategies of higher expected value. This paper has synthesized the process to apply set-based design to verification strategies and pointed to how evaluating dominance of strategies may be helpful to deal with the complexity resulting from the size of the problem.

Finally, this paper has also presented a refined model of the effects of rework activities in the expected value of a verification strategy. Although the model is still not sufficiently accurate of a real-life scenario, it improves prior work. Specifically, prior work relied on a predefined rework decision based on confidence thresholds. Instead, the proposed model considers that a rework activity is always initiated when a verification activity fails and considers its effect a function of the likelihood of such a verification result. In addition, and more importantly, it also incorporates the notion that rework may be needed at different levels of integration, requiring different levels of investment to solve the problem.

It should be noted that the effort is ongoing and is planned to be completed within the timeframe of the NPS Acquisition Research Program's "Dynamic Contracting of

Verification Activities by Applying Set-Based Design to the Definition of Verification Strategies” project.

References

Bernstein, J. I. (1998). *Design methods in the aerospace industry: Looking for evidence of set-based practices*. Cambridge, MA: Massachusetts Institute of Technology.

Engel, A. (2010). *Verification, validation, and testing of engineered systems*. Hoboken, NJ: John Wiley & Sons.

Rapp, S., Chinnam, R., Doerry, N., Murat, A., & Witus, G. (2018). Product development resilience through set-based design. *Systems Engineering, 21*(5), 490–500. doi:10.1002/sys.21449

Raudberget, D. (2010). Practical applications of set-based concurrent engineering in industry. *Journal of Mechanical Engineering, 56*(11), 685.

Salado, A. (2015). Defining better test strategies with tradespace exploration techniques and Pareto fronts: Application in an industrial project. *Systems Engineering, 18*(6), 639–658. doi:10.1002/sys.21332

Salado, A., & Kannan, H. (2018a). A mathematical model of verification strategies. *Systems Engineering, 21*, 583–608.

Salado, A., & Kannan, H. (2018b). *Properties of the utility of verification*. Paper presented at the IEEE International Symposium in Systems Engineering, Rome, Italy.

Salado, A., & Kannan, H. (2019). Elemental patterns of verification strategies. *Systems Engineering*. In press.

Salado, A., Kannan, H., & Farkhondehmaal, F. (2018). *Capturing the information dependencies of verification activities with Bayesian networks*. Paper presented at the Conference on Systems Engineering Research (CSER), Charlottesville, VA.

Singer, D. J., Doerry, N., & Buckley, M. E. (2009). What is set-based design? *Naval Engineers Journal, 121*(4), 31–43. doi:10.1111/j.1559-3584.2009.00226.x

Xu, P., & Salado, A. (2019). *A concept for set-based design of verification strategies.* Paper presented at the INCOSE International Symposium, Orlando, FL.

Acknowledgements & Disclaimer

This material is based upon work supported by the Acquisition Research Program under HQ00341810002. The views expressed in written materials or publications and/or made by speakers, moderators, and presenters do not necessarily reflect the official policies of the Department of Defense, nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Panel 11. Decision Making Within Defense Acquisition

Wednesday, May 8, 2019	
3:45 p.m. – 5:00 p.m.	**Chair: Brigadier General Michael Sloane, USA,** Program Executive Officer, Simulation, Training, and Instrumentation ***Case Study—Army's Search for a Better Uniform Camouflage Pattern*** Robert Mortlock, Naval Postgraduate School ***Survive, But Not Thrive? The Constraining Influence of Government Funding on Technology Start-Ups*** Jason Rathje, Stanford University ***An Analytic Model of Success for Information Technology Decision Making*** Thomas Clemons, K. C. Chang, and Sean Tzeng, George Mason University

Brigadier General Michael Sloane, USA—Brigadier General Sloane is the Program Executive Officer for Simulation, Training and Instrumentation (PEO STRI) in Orlando, Florida. PEO STRI executes a multi-billion dollar program annually, and is staffed by more than 1,000 military, government civilian and service support contractors. The organization also manages Foreign Military Sales programs which support more than 65 countries.

Prior to this assignment, Brigadier General Sloane served as the Assistant Program Executive Officer Enterprise Information Systems (PEO EIS) from December 2016 - June 2018. His responsibilities included the integration of the Army's Enterprise Resource Planning (ERP) systems as well as the migration of the ERPs in accordance with the Office of the Secretary of Defense and Army policies to the Defense Information Systems Agency data centers as part of the Army enclave. Prior to his position as Assistant PEO, Brigadier General Sloane served as the Chief of Staff to the Acting Assistant Secretary of the Army (Acquisition, Logistics and Technology).

Brigadier General Sloane was commissioned as an Army officer after earning a Bachelor of Business Administration from Columbus State University in Columbus, Georgia. He earned a Master of Business Administration from Webster University while attending the Command and General Staff College. In 2012, he graduated from the Industrial College of the Armed Forces (ICAF) with a Master of Science in National Resource Strategy and completed the Senior Acquisition Course.

Brigadier General Sloane has had operational assignments as a platoon leader and company executive officer while serving four years in the 24th Infantry Division (Mechanized). In the 24th ID, he deployed for Operations Desert Shield and Desert Storm, to Honduras for Joint Task Force 105 and to support Hurricane Andrew relief operations. His career includes a break in active duty service from 1993 to 1997 during which he worked in corporate industry and started a Limited Liability Corporation.

Upon recall to active duty in 1997, Brigadier General Sloane's military duties commenced with three years in the 10th Mountain Division (Light Infantry) serving as the Division Support Command S4 and as Commander, Bravo Company, 210th Forward Support Battalion. While commanding in the 10th Mountain Division, he deployed to the Balkans with the NATO-led multinational peacekeeping force, Stabilization Force 6.

In 2000, Brigadier General Sloane was assigned to Army Human Resources Command to serve as the Future Readiness Officer and an Assignment Officer. In 2003, following CGSC, he was assigned to the Missile Defense Agency's Terminal High Altitude Area Defense (THAAD) System Project Office as the Assistant Product Manager for Missile Development and later as Assistant Product Manager for THAAD System Test and Evaluation. In 2006, he was assigned to the Office of the Deputy Chief of Staff, G-1 as the lead Personnel Policy Integrator for the Acquisition, Chaplain and Judge Advocate General Corps. From 2008 to 2011, Brigadier General Sloane served in PEO Soldier as the Product Manager for Soldier Clothing and Individual Equipment then, following ICAF, he served three-and-a-half years as the Project Manager for Soldier Sensors and Lasers, starting in 2012.

Brigadier General Sloane's awards and decorations include Legion of Merits, Defense Meritorious Service Medal, Meritorious Service Medals, Army Commendation Medals, Joint Service Achievement Medal, Army Achievement Medals, Armed Forces Expeditionary Medal, Southwest Asia Service Medal (with three Bronze Service Stars), Global War on Terrorism/Service Medal, Humanitarian Service Medals, the NATO Badge, Saudi Arabia and Kuwait Liberation Medals, Parachutist Badge, Air Assault Badge, Ranger Tab, and the Army Staff Identification Badge.

Army's Search for a Better Uniform Camouflage Pattern—A
Case Study

Robert F. Mortlock, COL, USA (Ret.)—managed defense systems acquisition efforts for the last 15 of his 27 years in the U.S. Army, culminating in his assignment as the project manager for Soldier Protection and Individual Equipment in Program Executive Office for Soldier. He holds a PhD in chemical engineering from the University of California, Berkeley, an MBA from Webster University, an MS in national resource strategy from the Industrial College of the Armed Forces, and a BS in chemical engineering from Lehigh University. He is also a graduate from the Post-Doctoral Bridge Program of the University of Florida's Hough Graduate School of Business. [rfmortlo@nps.edu]

Abstract

The development, testing, and fielding of combat uniforms for United States (U.S.) soldiers offers project management (PM) professionals an opportunity to analyze how programs progress through the U.S. defense acquisition institution. This case study centers on the U.S. Army's decision to change the camouflage patterns on combat uniforms and equipment not only for soldiers stationed in war zones around the world, but also for soldiers in daily garrison operations stateside. The case study is broadly applicable to project managers, business managers, engineers, testers, and logisticians involved in PM within the private sector, while specifically targeting acquisition professionals within the government defense departments. Emphasis is placed on the development of critical thinking and analysis skills in the areas of stakeholder management and decision-making in a complex environment. The case is developed in two distinct parts. Part I allows PM professionals to analyze how to recommend a path forward to senior leaders with an increased chance of success of meeting desired objectives. Part II allows PM professionals to analyze how to recommend a set of options or courses of action for senior leaders to enable an informed, knowledge-based decision.

Executive Summary

The protection of American soldiers in combat was a top priority for senior leaders in the U.S. Army, DoD, and Congress. Camouflage on combat uniforms remained the most important contribution to the overall concealment of individual soldiers on the battlefield. Post-combat surveys from soldiers in Iraq and Afghanistan indicated that better camouflage on combat uniforms contributed to increased combat effectiveness. Soldiers recounted combat missions in which they were close enough to the enemy to hear conversations without being seen. This contributed to the tactical combat dominance of U.S. soldiers. Basically, the enemy cannot kill what they cannot see. Effective combat uniform camouflage remained a significant combat multiplier for soldiers—increasing mission accomplishment.

Army soldiers in Afghanistan faced diverse battlefield operating environments in combat operations. During a single mission, soldiers faced different terrains across various environmental backgrounds. Soldiers who wore combat uniforms and equipment with the universal camouflage pattern (UCP), a three-color digital pattern adopted by the Army in 2005, did not effectively blend into the diverse backgrounds typical during combat missions. The UCP colors were not earth tone and were generally too bright—making soldiers easy to detect and providing ineffective concealment. To specifically address combat operations in Afghanistan, the Army selected a commercially available camouflage pattern called MultiCam© to be used on uniforms and equipment for deploying soldiers to Afghanistan. The Army named the commercially available MultiCam© pattern the Operation Enduring Freedom Camouflage Pattern (OEF CP). In the meantime, the Army focused on a long-term camouflage strategy for soldier uniforms and equipment that would be effective across the diverse military operating environments and considered a family of three camouflage patterns—one suited for the woodland/jungle environments, one suited for desert/arid environments, and a transitional pattern suited for most other environments.

This combat uniform camouflage case study encourages critical analysis of the Army's combat camouflage uniform project at two key decision points. The case focuses on the development, testing, and procurement (also referred to as acquisition) of combat camouflage uniforms and equipment for U.S. Army soldiers. The case is interesting not only to project management (PM) professionals but also to warfighters who appreciate the importance of effective concealment for mission accomplishment and safety. Key project stakeholders are passionate about camouflage because it saves lives in combat, and all soldiers consider themselves subject matter experts on uniforms and camouflage—resulting in wide applicability. Decisions involved with the Army camouflage uniform effort involve a complex acquisition environment—requiring decision-making under uncertainty with consideration for performance, schedule, cost/affordability, legal risk, public perception, and congressional oversight. The combat uniform case study reinforces critical thinking in uncertain environments, documents lessons learned for sound PM for future application, and provides wide private-sector exposure to the complexities of public-sector acquisition and camouflage uniform development, testing, and manufacture in particular.

The case study data enables readers to become familiar with the history of Army combat camouflage uniforms, the basics of combat uniforms in general, and camouflage testing in particular. Readers of the case analyze alternative strategies for the Army path at two critical decision points. Both decisions involve critical thinking, stakeholder management, decision-making with uncertainty, and strategic leadership by focusing on the development of recommendations that decision-makers can use to make the most informed decision possible.

This case study centers on the U.S. Army's decision to change the camouflage patterns on combat uniforms and equipment not only for soldiers stationed in war zones around the world but also for soldiers in daily garrison operations stateside. The case is in two distinct parts. Part I allows PM professionals to analyze how to recommend a path forward to senior leaders with an increased chance of success of meeting desired objectives. Part II allows PM professionals to analyze how to recommend a set of options or courses of action for senior leaders to enable an informed, knowledge-based decision.

The case study has the following learning objectives:

- Develop the ability to critically analyze a project at key decision points by identifying advantages and disadvantages of various courses of action—critical thinking.
- Identify key stakeholders and understand their perspectives—stakeholder management.
- Develop a method to compare alternative strategies or courses of action for the decision-maker and defend a recommendation—decision-making with uncertainty or ambiguity.
- Compare alternative strategies and identify decision criteria used for the comparison—decision-making with uncertainty or ambiguity.
- Identify second-order considerations or consequences of the recommended strategies—strategic management/leadership.

Part I (Path Forward, Development of a Strategy, Fall 2013) of the case study focuses on the Army program manager as he prepares for meetings in the Pentagon after learning that the original Army contracting strategy has hit roadblock. The following are key questions to be addressed:

- Who are the key stakeholders in combat camouflage uniforms?
- Who is the ultimate decision-maker?
- How relevant was the test paradigm shift in this decision?
- What is a realistic test and evaluation strategy and schedule leading to decision in terms of key program and testing events planned by quarter?
- What options should the Army consider?
- What criteria should the Army use to compare options and then select the best path forward?

A key program management fundamental lessons learned from this part of the case includes not rushing to failure. Senior leaders and PMs must try to avoid the pitfalls of making rash decisions because the situation seems urgent. In this part of the case, it is probably best for the Army to take a strategic pause to let the congressional language become final, to and allow time to test additional patterns for which the government has data rights to avoid long-term affordability challenges.

Part II (Camouflage Decision, Winter 2013/Spring 2014) of the case focuses again on Army PMs as they present the testing results to Army senior leaders to support a path forward. The following are key questions to be addressed:

- Was $10 million spent over six years in the research, development, and testing of camouflaged uniforms a wise investment for the Army?
- Were the options considered by the Army appropriate? Were other viable options not considered?
- Was the source of funding (contingency funds or base budget funds) an important consideration? Why or why not?
- What were the affordability considerations for the Army in this decision?
- What were the important contractual and legal considerations in this decision?
- How should the Army compare the options and select the best path forward?

Some of the key program management fundamental lessons learned from this part of the case include the realization that even though performance and schedule are important, sometimes the preferred path forward must be decided by other criteria. PMs must bring together the information for the most informed decision possible. In this case, the PM has to understand the affordability/cost implications, legal risk, and the perspectives of key stakeholders including Congress, soldiers, U.S. Marine Corps, and the media.

“The rest of the story,” or what the Army actually did, can be studied not as the “right answer” but to provide closure for readers. Many paths often lead to similar end results for acquisition development programs. The case study itself provides the epilogue to the first key decision on how the Army proceeded when the strategy hit the contracting barrier. For the second key decision point, the Army selected a pattern and named it the Operational Camouflage Pattern (OCP) to emphasize that the pattern’s reach extends beyond

Afghanistan to other Army military operating environments. Because the alternative camouflage patterns all tested similarly, the decision came down to other considerations. The digital patterns that were based on the U.S. Marine Corps patterns (MARPATs) were never seriously considered because Army senior leaders were concerned about the following three things: strict literal compliance to the restrictions in the Fiscal Year 2014 National Defense Authorization Act (NDAA), the backlash from the U.S. Marine Corps leadership (who did not favor the Army leveraging the MARPATs), and the soldier/public perception of the Army choosing another "digital" pattern after the tepid response to the UCP adoption. The OEF CP pattern was not chosen because of affordability concerns. The Army continues to work on improving the force protection and concealment of soldiers through more effective camouflage for uniforms and equipment.

Operational Camouflage Case Study

Current Situation, October 2013

Colonel Bob Smith sat in his office at Fort Belvoir in total disbelief as he read an email from the contracting officer stating that a contract for the Army to purchase the camouflage pattern had never actually been accepted by the contractor. The email came after Colonel Smith asked the contracting officer to send a copy of the signed contract. The contracting officer's response was delayed by several weeks because Department of Defense (DoD) agencies were resuming normal operations after being shut down October 1–16, 2013, with most federal employees furloughed, because neither an appropriation act nor a continuing resolution was enacted for fiscal year 2014. On the Friday afternoon before the shutdown, the contracting office reported the successful award of a contract to Crye Precision LLC for their camouflage pattern, commercially known as MultiCam©. Due to significant Army senior leader and congressional interest, notification of the contract awarded was documented in significant activities reports to the chief of staff of the Army and secretary of the Army levels.

Now, Colonel Smith thought about how to notify the Army senior leaders that the contract was not awarded and that his team would have to develop options for the Army to consider going forward—both of these tasks were significant events considering the importance of the Army combat uniform camouflage decision. The Army had completed extensive combat uniform camouflage testing—testing that began in 2009 with reviews and a decision process that finally resulted in the selection of an acceptable camouflage pattern for Army combat uniforms (Program Manager Soldier Protection and Individual Equipment [PM SPIE], Program Executive Office Soldier [PEO Soldier], 2014c). Colonel Smith started to consider all the information needed to help Army senior leaders make an informed decision: the importance of camouflage to soldier force protection and mission effectiveness, camouflage testing basics, the history of the testing program, the status of soldier combat uniforms, and the affordability aspects of the decision. First things first—Colonel Smith asked his deputy to immediately draft a notice to inform senior leaders that the previously announced award of the contract was premature.

Background

It's Only Camouflage—How Important Can It Be on the Modern Battlefield?

The protection of American soldiers in combat was a top priority for senior leaders in the U.S. Army, DoD, and Congress. The DoD committed considerable resources and funding over the years in research and development, resulting in advanced materials and manufacturing processes (PM SPIE, PEO Soldier, 2014c). These investments increased the combat effectiveness of the soldiers and their units. Camouflage on combat uniforms remained the most important contribution to the overall concealment of individual soldiers on the battlefield. Reinforcing the importance of camouflage was the result of post-combat surveys from soldiers from duty in Iraq and Afghanistan, in which the majority of soldiers indicated that better camouflage on combat uniforms contributed to increased combat effectiveness. Anecdotal evidence from soldiers on the importance of camouflage came from recounted combat missions in which they were close enough to the enemy to hear conversations without being seen—particularly during night operations. This contributed to the dominance of U.S. soldiers and the "we own the night" tactical advantage of U.S. forces. Basically, the enemy cannot kill what they cannot see. Effective combat uniform camouflage remained a significant combat multiplier for soldiers.

Army soldiers in Afghanistan faced diverse battlefield operating environments in combat operations (see Figure 1). During a single mission, soldiers faced many different terrains across various environmental backgrounds. Each of these environmental backgrounds contained different earth-tone colors, which required different matching earth-tone colors in the combat uniform for it to effectively conceal a soldier from detection and/or observation. Soldiers who wore combat uniforms and equipment with the universal camouflage pattern (UCP), a three-color digital pattern adopted by the Army in 2005, did not effectively blend into the diverse backgrounds typical during combat missions. The UCP colors were not earth tone and were generally too bright—making soldiers easy to detect and providing ineffective concealment.

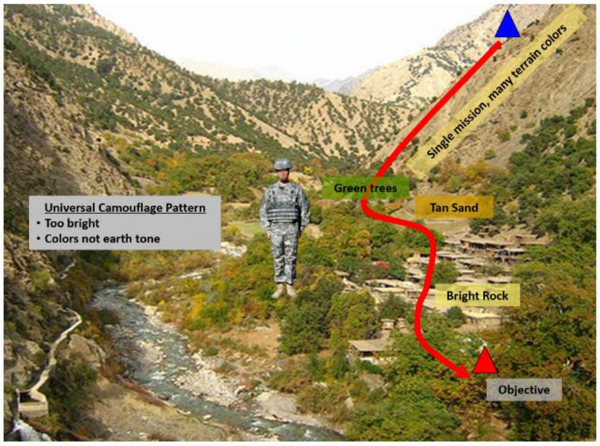


Figure 1. **Army Needed Better Camouflage**
(PM SPIE, PEO, 2013a)

The Army faced a critical question with respect to providing soldiers effective camouflage on combat uniforms and equipment: How many camouflage patterns should be adopted? Soldiers operating in diverse operating environments proved that the most effective camouflage pattern matched the colors of the background environment. A "chameleon" camouflage pattern eluded the Army due to low technological maturity level—basically it was just not feasible to have a combat uniform with chameleon camouflage that would change color on its own to fit into its environment. Logistical and affordability considerations limited the Army from adopting a specific camouflage pattern for every combat environment. The Army settled on a strategy considering three camouflage patterns—one suited for the woodland/jungle environments, one suited for desert/arid environments, and a transitional pattern suited for most other environments (PM SPIE, PEO, 2014c, 2013a; Office of the Secretary of the Army, 2009). In support of the combat uniform camouflage effort, the Army initiated an assessment of terrain throughout the globe. The Army Corps of Engineers classified the Army military operating environments across the combatant commands as 44% transitional, 37% woodland/jungle, and 19% desert/arid environments (Ryerson et al., 2012, 2013a, 2013b, 2013c, 2013d, 2013e). A woodland camouflage pattern would be very effective against backgrounds of darker brown and green colors and ineffective in dry arid regions (see Figure 2). On the other hand, a desert camouflage pattern would be very effective against backgrounds of lighter tan/sand colors and ineffective in woodland/jungle terrains. Finally, a transitional camouflage pattern would provide reasonable concealment against a broad range of environmental backgrounds. Seasonal considerations break down the woodland/jungle and transitional backgrounds even further to dormant (without leaves on trees) and verdant (with leaves on trees) classifications.

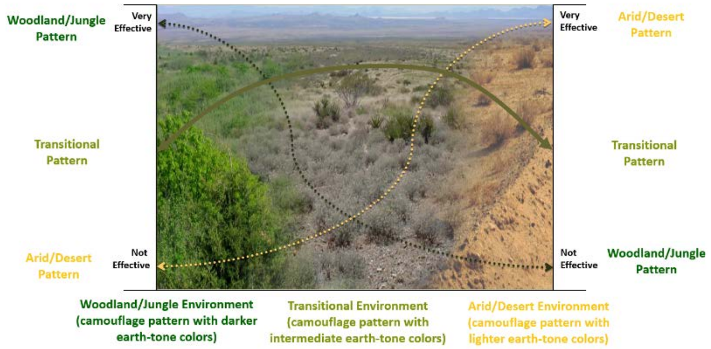

Woodland/Jungle Pattern
Very Effective
Transitional Pattern
Arid/Desert Pattern
Not Effective
Very Effective
Arid/Desert Pattern
Transitional Pattern
Not Effective
Woodland/Jungle Pattern
Woodland/Jungle Environment (camouflage pattern with darker earth-tone colors)
Transitional Environment (camouflage pattern with intermediate earth-tone colors)
Arid/Desert Environment (camouflage pattern with lighter earth-tone colors)

Figure 2. **Camouflage Effectiveness in Different Environments**
(PM SPIE, PEO Soldier, 2013a)

Camouflage Testing Basics

The Army recognized that advancing the science of combat uniform camouflage testing was vitally important to enabling knowledge-based decisions on the most effective camouflage pattern. It was acknowledged that it was unaffordable to field-test various camouflage patterns in every possible environment and background. To gain a statistically robust data set to support decision-making, the Army developed a test and evaluation strategy that involved a paradigm shift (see Figure 3). The strategy leveraged four mutually supporting lines of effort (PM SPIE, PEO Soldier, 2014a, 2013a). Technical development testing consisted of photo simulation for pattern selection and spectral reflectance measurements for performance insights. Operational field-testing with soldiers consisted of static observation tests for pattern performance confirmation and maneuver tests for both pattern performance confirmation and operational insights.

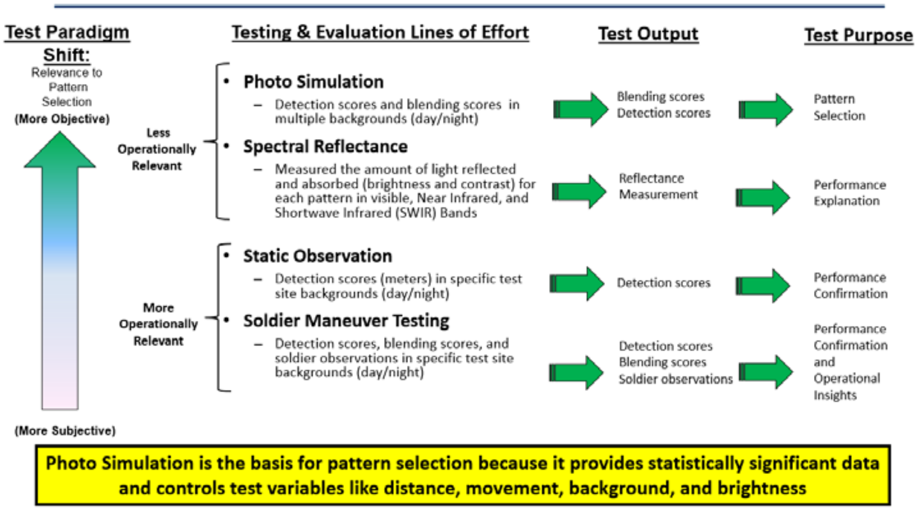

Test Paradigm Shift:
Relevance to Pattern Selection
(More Objective)
(More Subjective)
Testing & Evaluation Lines of Effort
Test Output
Test Purpose
Less Operationally Relevant
More Operationally Relevant
• Photo Simulation
– Detection scores and blending scores in multiple backgrounds (day/night)
• Spectral Reflectance
– Measured the amount of light reflected and absorbed (brightness and contrast) for each pattern in visible, Near Infrared, and Shortwave Infrared (SWIR) Bands
• Static Observation
– Detection scores (meters) in specific test site backgrounds (day/night)
• Soldier Maneuver Testing
– Detection scores, blending scores, and soldier observations in specific test site backgrounds (day/night)
Blending scores
Detection scores
Reflectance Measurement
Detection scores
Detection scores
Blending scores
Soldier observations
Pattern Selection
Performance Explanation
Performance Confirmation
Performance Confirmation and Operational Insights

Photo Simulation is the basis for pattern selection because it provides statistically significant data and controls test variables like distance, movement, background, and brightness

Figure 3. **Camouflage Test and Evaluation Strategy**
(PM SPIE, PEO Soldier, 2013a)

Normally, operationally realistic field-testing carried the most weight in decision-making over less operationally realistic developmental testing. For camouflage testing, however, a more extensive data set could be obtained if computer-based testing techniques were used in which soldiers observed photos of camouflaged uniforms in different backgrounds representing the Army's military operating environments (U.S. Army, Natick Soldier Research, Development, and Engineering Center [NSRDEC], 2009). The main effort for the test and evaluation strategy centered on the use of photo simulation to compare the effectiveness of camouflage patterns.

Two different criteria existed to compare the effectiveness of camouflage: detection and blending. Camouflage testing determined detection and blending scores for various camouflage patterns in relevant military operating environments. Detection is the ability to pick out the camouflage pattern measured at different distances, and blending is how well the camouflage pattern matches the background once detected at a specific range. Photo simulation evaluations allowed for collection of significant data in many backgrounds and controlled variables (such as distance, movement, background, and brightness) so the difference in detection and blending scores could be attributable to different camouflage patterns. The word "simulation" referred to the fact that the technique simulated soldiers being outside at the various sites by looking at computers screens of photos of soldiers in camouflage uniforms. Camouflage pattern selection criteria was based on both detection scores (at ranges to 450 meters during the day and to 250 meters at night) and blending scores (at 50 meters during the day and at 25 meters during the night; Hepfinger et al., 2010; Lacy & Rogers, 2014; U.S. Army, NSRDEC, 2004).

A Basic Overview of Army Combat Camouflage Uniforms

After basic initial entry training, the Army issued soldiers uniforms and other essential combat equipment classified as organization clothing and individual equipment (OCIE) and generally referred to as the soldier's clothing bag. Part of this issue to soldiers was the army combat uniform (ACU). The ACU was the uniform that soldiers wore in daily garrison operations when not deployed to combat operations. The ACU fabric was a 50–50 mix of cotton and nylon, and came with the universal camouflage pattern (UCP), selling in the Military Clothing Store for about $90 for a coat and trouser set (PM SPIE, PEO Soldier, 2014c). After they wore out, soldiers used their clothing replacement allowance to buy new sets of uniforms. Examples of OCIE included the seven-layer Generation III Extended Cold Weather Clothing System (ECWCS), the field pack or rucksack (part of the modular lightweight load-carrying equipment [MOLLE]), and the ballistic vests (part of the improved outer tactical vests [IOTV])—all issued with the UCP.

Beginning in mid-2005, the Army recognized the importance of protecting soldiers from battlefield hazards and included specific uniform requirements for protection against insects (resulting in permethrin treatment) and fire or flame (resulting in flame-resistant fabrics). When soldiers deployed to combat, the Army issued soldiers the Flame Resistant Army Combat Uniform (FRACU) with the UCP. The FRACU was made of 65% rayon, 25% para-aramid, and 10% nylon. The price of a FRACU set of coat and trousers averaged about $180 (PM SPIE, PEO Soldier, 2014c). Additionally, soldiers received the Flame Resistant Environment Ensemble (FREE)—the flame-retardant version of the ECWCS. Soldiers did not normally deploy with the clothing bag-issued ACU and ECWCS—those were for daily wear in garrison operations and in training. In 2011, the Army issued soldiers deploying to Afghanistan for Operation Enduring Freedom (OEF) the FRACUs and OCIE with the OEF Camouflage Pattern (OEF CP).

Figure 4 displays a pictorial representation of the uniforms soldiers would typically have worn in the summer of 2013 around the world. Soldiers wore the ACU with UCP in most regions of the world, except in the Middle East. Soldiers wore the FRACU with UCP when deployed from combat operations in Iraq and Kuwait, while soldiers supporting combat operations in OEF wore the FRACU in OEF CP.

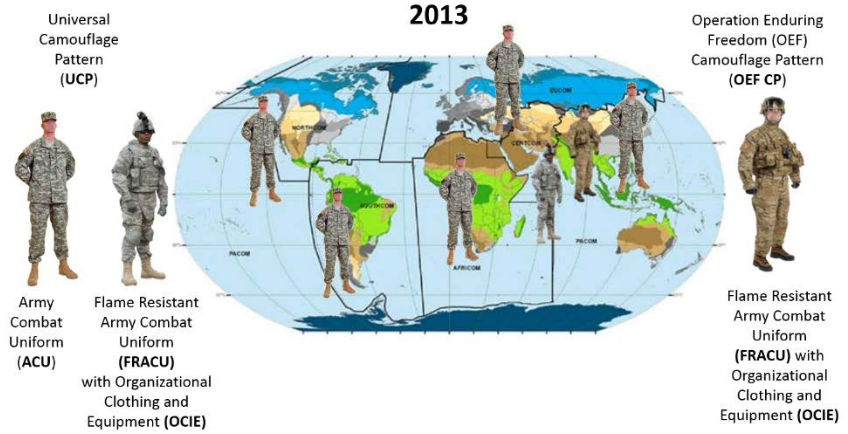
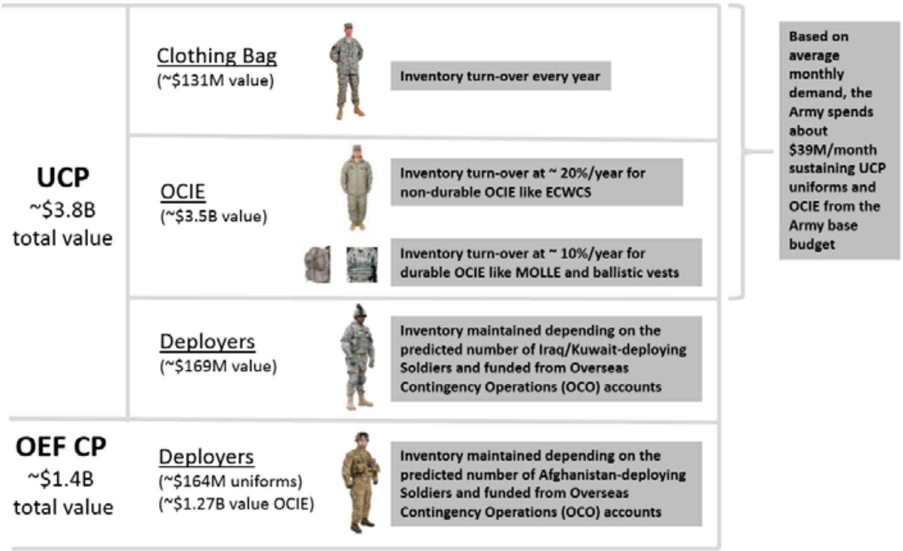

2013
Universal Camouflage Pattern (UCP)
Operation Enduring Freedom (OEF) Camouflage Pattern (OEF CP)
NORTHCOM
EUCOM
CENTCOM
SOUTHCOM
AFRICOM
PACOM
PACOM
Army Combat Uniform (ACU)
Flame Resistant Army Combat Uniform (FRACU) with Organizational Clothing and Equipment (OCIE)
Flame Resistant Army Combat Uniform (FRACU) with Organizational Clothing and Equipment (OCIE)

Figure 4. **Common Operation Picture for Army Combat Uniforms**
(PM SPIE, PEO Soldier, 2013)

The Army remained very cognizant of the value of the combat uniforms and OCIE worn by soldiers and in the inventory. For example, based on the number of active, reserve, and National Guard soldiers both non-deployed and deployed, the ACUs worn by soldiers in their clothing bag valued about $131 million and turned over every year (PM SPIE, PEO Soldier, 2013a, 2014c). The value of OCIE worn by soldiers or in inventory with UCP totaled about $3.5 billion and turned over every 5–10 years depending on the durability of the items. Deploying soldiers to Iraq and Kuwait had another $170 million worth of UCP uniforms and OCIE. Uniforms and OCIE with the UCP totaled over $3.8 billion in value (see Figure 5). To support soldiers deploying to Afghanistan, the Army maintained uniforms and OCIE with the OEC CP with a value of about $1.4 billion. Based on the average monthly demand, the Army spent approximately $39 million per month sustaining UCP uniforms and OCIE from the Army base operations and maintenance budget for an Army of approximately one million soldiers (active, guard, and reserve components; PM SPIE, PEO Soldier, 2013a, 2014c).



UCP
~$3.8B
total value

Clothing Bag
(~$131M value)

Inventory turn-over every year

OCIE
(~$3.5B value)

Inventory turn-over at ~ 20%/year for non-durable OCIE like ECWCS

Inventory turn-over at ~ 10%/year for durable OCIE like MOLLE and ballistic vests

Deployers
(~$169M value)

Inventory maintained depending on the predicted number of Iraq/Kuwait-deploying Soldiers and funded from Overseas Contingency Operations (OCO) accounts

OEF CP
~$1.4B
total value

Deployers
(~$164M uniforms)
(~$1.27B value OCIE)

Inventory maintained depending on the predicted number of Afghanistan-deploying Soldiers and funded from Overseas Contingency Operations (OCO) accounts

Based on average monthly demand, the Army spends about $39M/month sustaining UCP uniforms and OCIE from the Army base budget

Figure 5. **The Value of Camouflaged Army Uniforms and Equipment**
(PM SPIE, PEO Soldier, 2013a)

Army Combat Uniform Evolution

Figure 6 presents a brief recent history of Army combat uniforms since the adoption of the ACU with the UCP. In 2005, the Army adopted the ACU to replace the battle dress uniform (BDU) with the woodland camouflage pattern and desert camouflage uniform (DCU) with the desert camouflage pattern. The ACU was produced with the UCP—a three-color (urban gray, desert sand, and foliage green) digital pattern. The Army wanted a single combat uniform design with a single camouflage pattern. In camouflage blending tests (day and night) using photo simulation techniques, UCP provided the best average performance across desert, woodland, and urban environments compared to 10 other patterns. These patterns were marine pattern (MARPAT) desert, MARPAT woodland, Scorpion (a pattern developed by Crye Precision LLC under a contract with the Army), desert brush, desert track, desert/urban track, standard desert (DCU), woodland track, standard woodland (BDU), and woodland brush. The Army's decision to adopt a digital pattern was influenced by the success of the U.S. Marine Corps' digital patterns—MARPAT woodland and MARPAT desert. Ultimately, in testing, UCP provided better or equal concealment than other patterns in urban and desert terrains—obviously very important to the Army embroiled in combat operations in Iraq (U.S. Army, NSRDEC, 2004, 2005).

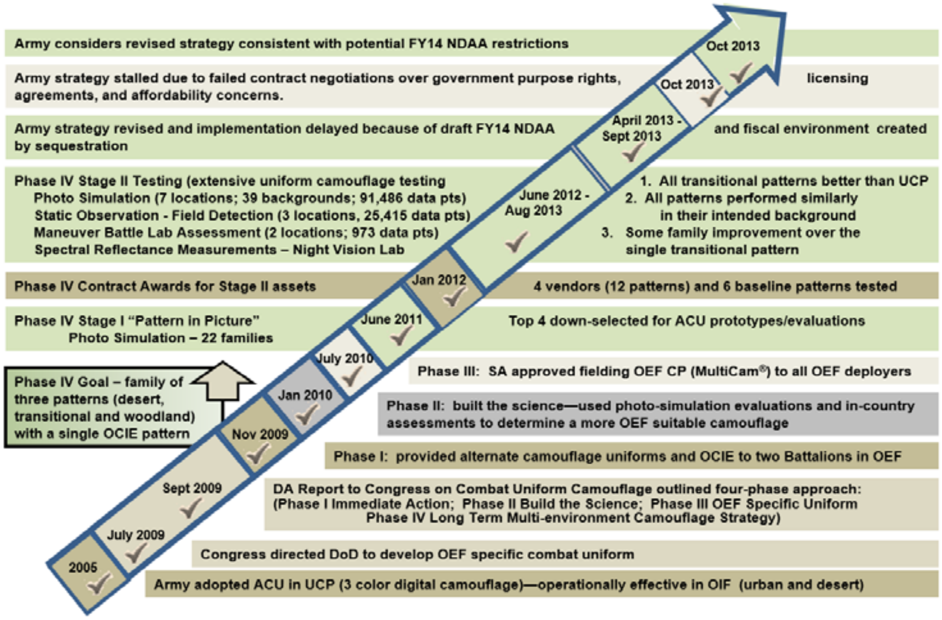

Army considers revised strategy consistent with potential FY14 NDAA restrictions
Oct 2013
Army strategy stalled due to failed contract negotiations over government purpose rights, licensing agreements, and affordability concerns.
Oct 2013
Army strategy revised and implementation delayed because of draft FY14 NDAA and fiscal environment created by sequestration
April 2013 - Sept 2013
Phase IV Stage II Testing (extensive uniform camouflage testing
Photo Simulation (7 locations; 39 backgrounds; 91,486 data pts)
Static Observation - Field Detection (3 locations, 25,415 data pts)
Maneuver Battle Lab Assessment (2 locations; 973 data pts)
Spectral Reflectance Measurements – Night Vision Lab
June 2012 - Aug 2013
1. All transitional patterns better than UCP
2. All patterns performed similarly in their intended background
3. Some family improvement over the single transitional pattern
Phase IV Contract Awards for Stage II assets
Jan 2012
4 vendors (12 patterns) and 6 baseline patterns tested
Phase IV Stage I "Pattern in Picture"
Photo Simulation – 22 families
June 2011
Top 4 down-selected for ACU prototypes/evaluations
July 2010
Phase III: SA approved fielding OEF CP (MultiCam®) to all OEF deployers
Phase IV Goal – family of three patterns (desert, transitional and woodland) with a single OCIE pattern
Jan 2010
Phase II: built the science—used photo-simulation evaluations and in-country assessments to determine a more OEF suitable camouflage
Nov 2009
Phase I: provided alternate camouflage uniforms and OCIE to two Battalions in OEF
Sept 2009
DA Report to Congress on Combat Uniform Camouflage outlined four-phase approach: (Phase I Immediate Action; Phase II Build the Science; Phase III OEF Specific Uniform Phase IV Long Term Multi-environment Camouflage Strategy)
July 2009
Congress directed DoD to develop OEF specific combat uniform
2005
Army adopted ACU in UCP (3 color digital camouflage)—operationally effective in OIF (urban and desert)

Figure 6. **Army Camouflage Uniform Timeline**
(Lacey & Rogers, 2014; PM SPIE, PEO Soldier, 2013a; U.S. Army, NSRDEC, 2005, 2012)

From the adoption of the ACU in 2005 until 2009, the Army received overwhelmingly negative feedback from soldiers in combat operations in Afghanistan about the suitability of the FRACUs in UCP for the diverse Afghan backgrounds, terrains, and environments (see Figure 1). As a result, in the fiscal year (FY) 2009 Supplemental Appropriations Act, Congress directed the Army to take immediate action to provide effective camouflage for personnel deployed to Afghanistan (U.S. House of Representatives, 2009). In September 2009, the Army submitted a report to Congress on combat uniform camouflage that outlined a four-phased approach: Phase I—Immediate Action, Phase II—Build the Science, Phase III—OEF Specific Camouflage, and Phase IV—Army Combat Uniform Decision for a Long Term Multi-Environment Camouflage (Office of the Secretary of the Army, 2009).

In November 2009, the Army completed Phase I by fielding two Army battalions (approximately 2,000 soldiers) with uniforms and OCIE in two different patterns. One camouflage pattern was Universal Camouflage Pattern-D (UCP-D)—a variant of UCP with coyote brown color added and less sand color—and the other pattern was commercial camouflage called MultiCam© produced by Crye Precision LLC. MultiCam©—a seven-color pattern that was in use at the time with U.S. Special Forces in Afghanistan—was a variation of the original Scorpion pattern considered by the Army earlier in the UCP decision (PM SPIE, PEO Soldier, 2013a, 2014c).

From November 2009 to January 2010, the Army conducted Phase II, which involved soldier feedback of the two fielded patterns (MultiCam© and UCP-D) as well as photo simulation (pattern-in-picture) evaluations by soldiers of six camouflage patterns (UCP, MultiCam©, UCP-D, Mirage, Desert Brush, and a Navy pattern referred to as AOR2), inserted into photographs of eight different OEF sites. Soldiers overwhelmingly preferred both MultiCam© and UCP-D with an edge in preference toward MultiCam© (PM SPIE, PEO Soldier, 2013a, 2014c).

In February 2010, initiating Phase III, the Army selected MultiCam© as the pattern to be used on the FRACU and OCIE for deploying soldiers to Afghanistan. The Army named the commercially available MultiCam© pattern as the OEF camouflage pattern (OEF CP). Because schedule and speed of delivery was critical, the Army encouraged Crye to enter separate licensing agreements with the companies that printed the OEF CP on FRACUs and OCIE. In July 2010, the Army began fielding uniforms and OCIE in the OEF CP to deploying OEF soldiers. The Army ended up paying about a 10% premium on every uniform or piece of camouflaged equipment that was camouflaged with OEF CP compared to uniforms equipment with UCP (PM SPIE, PEO Soldier, 2013a, 2014c). At the time, schedule and getting updated camouflaged uniforms and equipment to field as quickly as possible trumped affordability concerns—especially considering that uniforms for combat operations in Afghanistan was funded by overseas contingencies operations (OCO) accounts.

In December 2010, the Maneuver Center of Excellence (MCoE) outlined an 18-month competitive effort to lead a camouflage integrated product team (IPT) through the Phase IV effort for the Army's selection of the long-term combat uniform and OCIE camouflage strategy to be effective in desert/arid, transitional, and woodland/jungle environments. The goal was to present the results to Army leadership in the fall of 2012 for a decision (Office of the Secretary of the Army, 2009).

From January 2011 to June 2011, the Army scoped the Phase IV camouflage effort. Based on work performed by the Natick Soldier Research Development and Engineering Center (NSRDEC) completed in 2009, the Army knew that environmentally specific camouflage patterns outperformed (meaning provided more effective concealment) a single "universal" pattern (U.S. Army, NSRDEC, 2004, 2005, 2009, 2012). The objective of Phase IV was to develop a "family" of three uniform camouflage patterns with a single coordinated pattern for OCIE to provide effective concealment across the globe in woodland/jungle, transitional, and desert/arid environments. A total of 22 family submissions from industry and the government competed in the first stage of Phase IV—18 family submissions were found be technically acceptable. These families of patterns participated in "pattern in picture" blending photo simulation evaluation. The patterns were judged based on the best legacy patterns in the Defense Department inventory (desert vs. a Navy pattern called AOR1, transitional vs. OEF CP, and woodland vs. a Navy pattern called AOR2) with family scores equally weighting the woodland, transitional, and desert environments. Five families of patterns (four commercial vendors and one NSRDEC submission) performed as well as or better than the legacy family of patterns. The four down-selected vendors included Crye Precision LLC, Kryptek Inc., Atlantic Diving Supply (ADS) Inc., and Brookwood Companies Inc. It is noteworthy that three patterns were visually similar in appearance: OEF CP (a baseline pattern), the transitional pattern proposed by Crye, and the transitional pattern submitted by NSRDEC named ScorpionW2. Each of these patterns was developed, changed, and optimized independently from the same base pattern called Scorpion—a pattern developed by Crye in the early 2000s under contract with the U.S. Army. All three patterns performed similarly in testing which served as a built-in, internal verification of the validity of the testing. At the time, even though the NSRDEC family performed well in source selection pattern-in-picture photo simulation testing, the Army decided not to continue to allow the NSRDEC family of patterns to participate in Stage II Phase IV testing because the family of patterns was not of consistent matching geometric shapes—one of the criteria established by the Army and required in the contracts with the four commercial vendors (PM SPIE, PEO Soldier, 2013a, 2014c).

In January 2012, Phase IV contracts were awarded to the four down-selected vendors to produce fabric for test articles (both uniforms and OCIE) for the second stage of Phase IV, which would include field testing, extensive photo simulation evaluations, and lab testing (Natick Contracting Division, U.S. Army Contracting Command—APG, 2012a, 2012b, 2012c, 2012d). The contracts with each of the four vendors were firm fixed price (FFP) contracts, with periods of performance not to exceed 30 months to supply the Army with 1,000 yards of fabric to be used by the Army to fabricate testing uniforms and OCIE under separate "cut and sew" contracts. The contracts included FFP options for the government to procure the non-exclusive license rights for each of the proposed camouflage patterns. The competitive range to buy the license rights from the four vendors for a single camouflage pattern ranged from $25,000 to $2.1 million. Crye offered the set of patterns for $600,000 ($200,000 each for three patterns—woodland, desert, and transitional/OCIE), ADS offered the set for $533,000 ($133,000 each for four patterns—woodland, desert, transitional, and OCIE), Brookwood offered the set for $100,000 ($25,000 each for four patterns—woodland, desert, transitional, and OCIE), and Kryptek offered the set for $6.3 million ($2.1 million each for three patterns—woodland, desert, and transitional/OCIE) (Natick Contracting Division, U.S. Army Contracting Command–APG, 2012a, 2012b, 2012c, 2012d). Each of the four vendors signed a non-exclusive license agreement which provided the Army the option to obtain (for a single lump sum) the rights to use the material for the production of patterns for printing on an unlimited number of uniforms, individual equipment, and unit level equipment for U.S. government purposes (e.g., Army, Navy, Marine Corps, Air Force, and Coast Guard, including their active and reserve components) excepting foreign military sales with successive renewable 10-year periods.

From July 2012 to March 2013, the Army conducted the most extensive uniform camouflage testing ever undertaken. The 12 commercial vendors' patterns (each of the four vendors had a woodland, transitional, and desert pattern along with a matching transitional OCIE pattern) and six reference patterns (UCP, OEF CP, MARPAT-W, MARPAT-D, AOR1, and AOR2) were printed on fabric, and the fabric was assembled into uniforms and OCIE (see Figure 7).

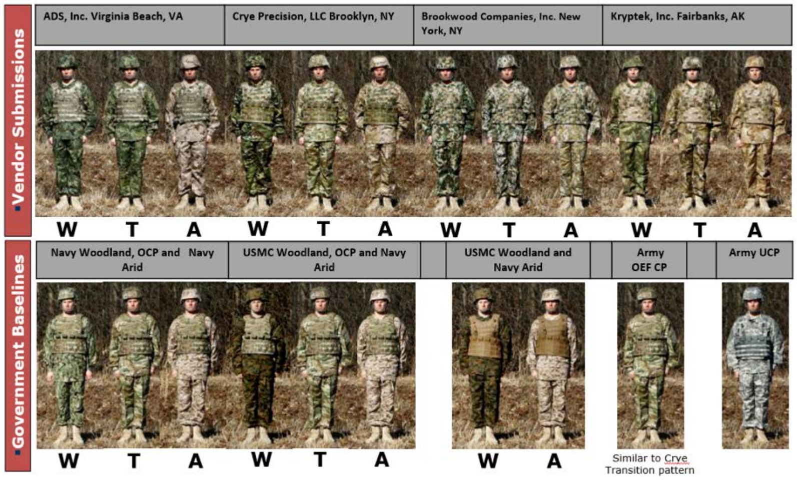

Vendor Submissions
ADS, Inc. Virginia Beach, VA
Crye Precision, LLC Brooklyn, NY
Brookwood Companies, Inc. New York, NY
Kryptek, Inc. Fairbanks, AK
W T A W T A W T A W T A
Government Baselines
Navy Woodland, OCP and Navy Arid
USMC Woodland, OCP and Navy Arid
USMC Woodland and Navy Arid
Army OEF CP
Army UCP
W T A W T A W A
Similar to Crye Transition pattern

Figure 7. **Phase IV Camouflage Patterns Tested**
(Mazz & Rowe, 2013; Rogers et al., 2013)

Note. W refers to woodland, T refers to transitional, and A refers to arid.

The photo simulation evaluations collected 91,486 data points in detection and blending tests (both day and night) using 39 different backgrounds from seven global locations. Field tests for static observations detections were conducted at three different locations, resulting in the collection of an additional 25,415 data points. Operational field tests with force-on-force soldiers were conducted at two locations, gathering another 973 data points (Mazz & Rowe, 2013; PM SPIE, PEO Soldier, 2013a, 2014c; Rogers et al., 2013).

The results of this extensive testing showed that all the vendor patterns in their intended backgrounds performed better than UCP—confirming the Army's intent to replace UCP. All the vendors patterns performed similarly in their intended backgrounds—this "tight shot" group gave the Army many options and confirmed that overall pattern colors and brightness was much more important than pattern design when assessing concealment effectiveness. There was slight improvement in effectiveness of a family of patterns in their intended backgrounds over the performance of a single transitional pattern across the three background classes; however, the operational relevance of this improved performance could not be quantified.

In May 2013, Army senior leaders approved the expanded use of OEF CP to replace UCP across the Army and the purchase of the non-exclusive government license rights to one of the competing vendors' patterns (the Crye transitional pattern that was very similar and visually indistinguishable from OEF CP) offered as an option in the Phase IV contract (PM SPIE, PEO Soldier, 2013b). Because all of the vendor patterns performed similarly in testing, the decision was based on other considerations, primarily affordability—the Army could leverage existing inventories of OEF CP OCIE and reduce the overall implementation costs to the Army.

However, the announcement of the decision and implementation was delayed. Army senior leaders were hesitant to announce a uniform change decision during a time of intense budget pressure and with the threat of sequestration looming. More importantly, the draft FY 2014 National Defense Authorization Act (NDAA) was released, and it potentially limited the Army's camouflage flexibility by prohibiting any new camouflage patterns unless all services adopted the new pattern. At the time, it was unclear whether the camouflage patterns tested in the Phase IV effort would potentially violate the NDAA restrictions.

In August 2013, to avoid the threat of protests by Phase IV vendors and subsequent lengthy contractual challenges and to avoid potential violations of the new statutory restrictions in the pending NDAA, the Army changed its contracting strategy to pursue a sole-source contract for the non-exclusive license rights (i.e., government purpose rights) to OEF CP and to delay exercising any remaining Phase IV contract options until the FY14 NDAA language was final (PM SPIE, PEO Soldier, 2013c). The vendor, Crye Precision LLC, indicated to the Army that the price for OEF CP would be similar to the price offered to the Army for the transitional pattern non-exclusive license rights in the Phase IV contract.

In October 2013, Crye Precision LLC balked at the terms of the contract proposed by the Army for OEF CP. The contract terms for the non-exclusive license rights were identical to the Phase IV contract option terms. Crye Precision LLC now wanted considerably more money for OEF CP than they accepted for their transitional pattern.

Part I: Path Forward, Development of a Strategy, Fall 2013

All this information swirled around in Colonel's Smith head as he prepared to meet in the Pentagon with Army senior leaders. Fortunately, for Colonel Smith, the chief of staff of the Army's Office wanted the following specifically addressed in the meeting scheduled for December 2013:

- How did this happen? How was a contract reported as signed that was not actually signed? What was the impact of the pending NDAA restrictions and how would the Army keep Congress informed? What was the impact on the Phase IV contracts?

- What was the schedule and a path toward an Army decision? What were the camouflage options, as well as key program and testing events considering the performance, cost, and schedule implications?
- What were the risks associated with this camouflage decision?

Based on the guidance from leadership, Colonel Smith and his team put together some options for the Army to consider (PM SPIE, PEO Soldier, 2014c):

- Option 1: Continue to negotiate with Crye for the non-exclusive rights for OEF CP. The initial price quoted started at $65 million but reduced to a lump sum of $24 million or 1% royalty on the price of each camouflaged item.
- Option 2: Exercise the Phase IV contract option for non-exclusive rights to the Crye transitional pattern.
- Option 3: Renegotiate all the Phase IV contract options for the non-exclusive rights for the patterns with all four vendors and select a pattern after the renegotiations.
- Option 4: Take a strategic pause and consider existing government patterns and patterns in which the government has license rights—for example, the NSRDEC pattern ScorpionW2.

Colonel Smith asked his team if there were any other options and what the decision criteria would be to compare these courses of action. Performance of the patterns remained the Army's most important criteria. However, cost/affordability was important, as well as schedule, congressional considerations (adherence to law), and litigation considerations such as the chance of protests and lawsuits challenging intellectual property rights to potential patent, copyright, and trademark issues.

Colonel Smith realized this would not be an easy set of meetings at the Pentagon. Despite the importance of combat uniform camouflage, efforts to change camouflage face the challenges that all programs within the DoD face: a complex, bureaucratic defense acquisition institution (Mortlock, 2016). Any decision to change Army camouflage crosses multiple chains of command with different decision-makers because it affects both uniforms and equipment. Uniform changes are approved by the chief of staff of the Army (CSA)—and sometimes the secretary of the Army (SecArmy), if there is intense congressional, public, or media interest—after an approval recommendation from the Army Uniform Board. But camouflage also goes on organizational clothing and individual equipment (OCIE), and each piece of soldier kit (cold weather clothing, rucksacks, weapons, bags for night vision sights, etc.) may have a different program decision-maker—either a program executive officer or the Army acquisition executive (AAE), depending on the acquisition category. Colonel Smith labored over how to pull together this information into a decision and what recommendation he would make when invariably asked by Army senior leaders. What should the Army decide?

Exhibit 1. Part I Case Study Discussion Questions

- Who are the key stakeholders in combat camouflage uniforms?
- Who is the ultimate decision-maker?
- How relevant was the test paradigm shift in this decision?
- What is a realistic test and evaluation strategy and schedule leading to decision in terms of key program and testing events planned by quarter?
- What options should the Army consider?
- What criteria should the Army use to compare options and then select the best path forward?

Part II: Camouflage Decision, Winter 2013/Spring 2014

Following a series of meetings in the Pentagon with Army senior leaders, the chief of staff of the Army issued the following guidance: Delay any immediate decision, ensure all options for the Army moving forward were rigorously tested, ensure the options considered met the intent of the NDAA by pulsing the congressional professional staff members, and provide an update to the secretary of the Army (PM SPIE, PEO Soldier, 2013d). The secretary of the Army subsequently approved the testing of transitional pattern alternatives for March 2014 with an anticipated decision pending successful and positive testing results in April 2014 (see Figure 8; PM SPIE, PEO Soldier, 2014a).

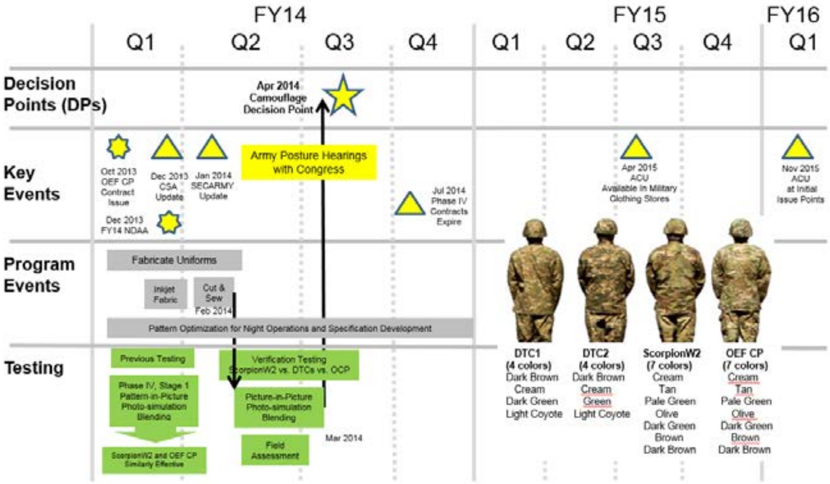

FY14
FY15
FY16
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Decision Points (DPs)
Apr 2014 Camouflage Decision Point
Key Events
Oct 2013 OEF CP Contract Issue
Dec 2013 CSA Update
Jan 2014 SECARMY Update
Army Posture Hearings with Congress
Dec 2013 FY14 NDAA
Jul 2014 Phase IV Contracts Expire
Apr 2015 ACU Available In Military Clothing Stores
Nov 2015 ACU at Initial Issue Points
Program Events
Fabricate Uniforms
Inkjet Fabric
Cut & Sew
Feb 2014
Pattern Optimization for Night Operations and Specification Development
Testing
Previous Testing
Phase IV, Stage 1 Pattern-in-Picture Photo-simulation Blending
ScorpionW2 and OEF CP Similarly Effective
Verification Testing ScorpionW2 vs. DTCs vs. OCP
Picture-in-Picture Photo-simulation Blending
Field Assessment
Mar 2014
DTC1 (4 colors) Dark Brown Cream Dark Green Light Coyote
DTC2 (4 colors) Dark Brown Cream Green Light Coyote
ScorpionW2 (7 colors) Cream Tan Pale Green Olive Dark Green Brown Dark Brown
OEF CP (7 colors) Cream Tan Pale Green Olive Dark Green Brown Dark Brown

Figure 8. **Approved Revised Army Plan**
(PM SPIE, PEO Soldier, 2014a)

After being reprimanded for lack of proper program oversight and damaging the reputation of Army acquisition leaders in the Pentagon, Colonel Smith led his team to execute yet another revised strategy for combat uniform camouflage testing. In December 2013, the FY14 NDAA became final and officially prohibited the services from adopting new camouflage patterns unless all the services adopted the new pattern (U.S. Congress, 2013). This new law restricted the number camouflage patterns considered going forward. The intent of the new strategy was to consider alternatives to OEF CP that provided equivalent or better performance, were affordable/fiscally responsible to implement, and were in compliance with the FY14 NDAA. The testing included three baseline reference patterns (UCP, MARPAT Woodland, and MARPAT Desert), OEF CP, and viable OEF CP alternatives. These alternatives were the ScorpionW2 pattern and two digital transitional camouflage patterns (referred to as DTC1 and DTC2—patterns based on MARPAT but with four earth-tone based colors; see Figure 9). The Army had a series of meetings with congressional members who sponsored the NDAA legislation and professional staff members who wrote the actual language to ensure the patterns considered were within the intent of the law. Congressional leaders considered the DTC1 and DTC2 patterns in a “gray area” of the new restrictions and were noncommittal if these patterns met the intent of the law. Nevertheless, the Army decided to test these patterns along with the other patterns.

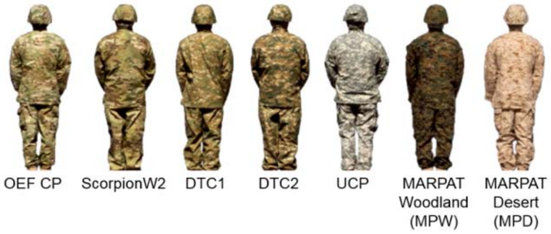
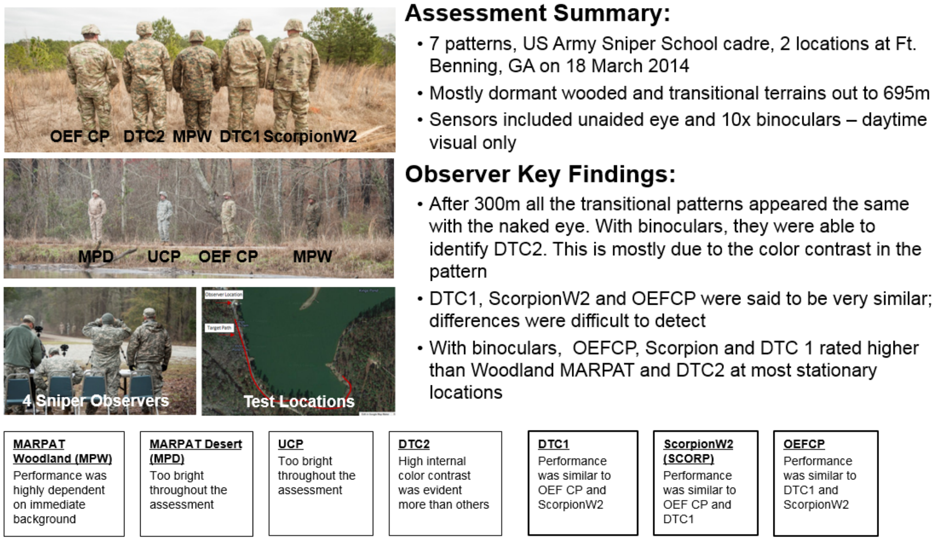


Figure 9. **Patterns Tested by the Army at Fort Benning in April 2014**
(Mazz, 2014; PM SPIE, PEO Soldier, 2014b)

In April 2014, the Army tested alternative transitional patterns at Fort Benning in operational field tests with U.S. Army Sniper School Cadre and in photo simulation assessments using soldiers from the 75th Ranger Regiment (see Figures 10 and 11). The testing to support an Army decision was rigorous and met the intent of the Army CSA. The testing involved used sniper experts to assess the operational relevance of the patterns in operational field tests and 106 soldiers as observers of the patterns in 46 separate backgrounds in photo simulation evaluations—collecting 19,474 data points (Mazz, 2014; PM SPIE, PEO Soldier, 2014b).



Assessment Summary:

- 7 patterns, US Army Sniper School cadre, 2 locations at Ft. Benning, GA on 18 March 2014
- Mostly dormant wooded and transitional terrains out to 695m
- Sensors included unaided eye and 10x binoculars – daytime visual only

Observer Key Findings:

- After 300m all the transitional patterns appeared the same with the naked eye. With binoculars, they were able to identify DTC2. This is mostly due to the color contrast in the pattern
- DTC1, ScorpionW2 and OEFCP were said to be very similar; differences were difficult to detect
- With binoculars, OEFCP, Scorpion and DTC 1 rated higher than Woodland MARPAT and DTC2 at most stationary locations

MARPAT Woodland (MPW)
Performance was highly dependent on immediate background

MARPAT Desert (MPD)
Too bright throughout the assessment

UCP
Too bright throughout the assessment

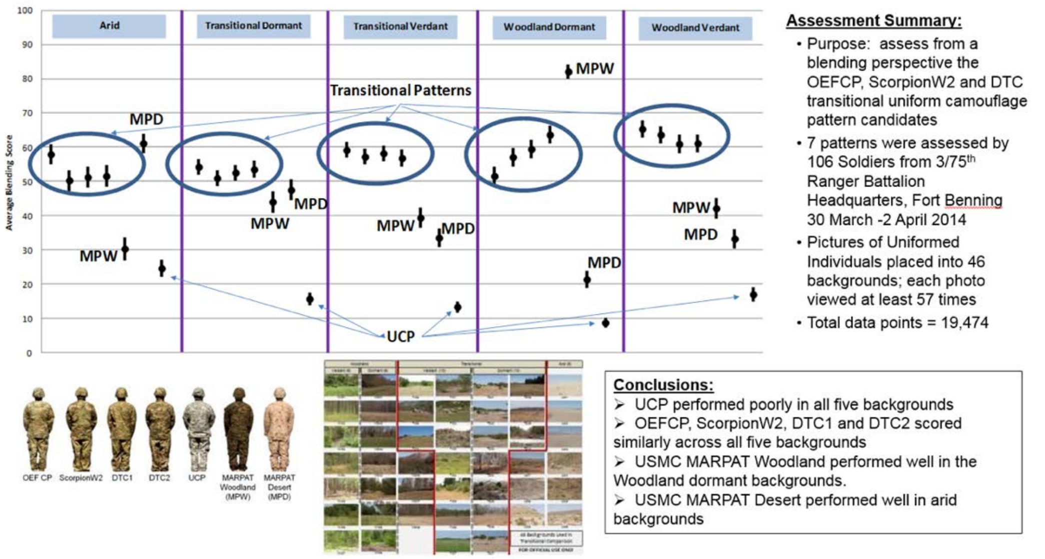
DTC2
High internal color contrast was evident more than others

DTC1
Performance was similar to OEF CP and ScorpionW2

ScorpionW2 (SCORP)
Performance was similar to OEF CP and DTC1

OEFCP
Performance was similar to DTC1 and ScorpionW2

Figure 10. **Operational Field Test Results**
(Mazz, 2014; PM SPIE, PEO Soldier, 2014b)



Assessment Summary:

- Purpose: assess from a blending perspective the OEFCP, ScorpionW2 and DTC transitional uniform camouflage pattern candidates
- 7 patterns were assessed by 106 Soldiers from 3/75th Ranger Battalion Headquarters, Fort Benning 30 March -2 April 2014
- Pictures of Uniformed Individuals placed into 46 backgrounds; each photo viewed at least 57 times
- Total data points = 19,474

Conclusions:

➢ UCP performed poorly in all five backgrounds
➢ OEFCP, ScorpionW2, DTC1 and DTC2 scored similarly across all five backgrounds
➢ USMC MARPAT Woodland performed well in the Woodland dormant backgrounds.
➢ USMC MARPAT Desert performed well in arid backgrounds

Figure 11. **Photo Simulation Test Results**
(Mazz, 2014; PM SPIE, PEO Soldier, 2014b)

From the results shown in Figures 10 and 11, the Army came to the following conclusions: UCP performed poorly in all backgrounds (confirming prior results); OEF CP, ScorpionW2, DTC1, and DTC2 scored similarly across all background types; USMC MARPAT woodland performed well in woodland dormant backgrounds; and USMC MARPAT desert performed well in arid environments. The results confirmed that there was a "tight shot" group for the effectiveness and performance of the transitional patterns. The Army decision would probably come down to other considerations like affordability, cost, implementation and execution ease, schedule, contracting challenges, and intellectual property rights concerns (potential patent, trademark, and copyright challenges).

Again, Colonel Smith assembled his team to consider the following options for CSA and SecArmy to consider (PM SPIE, PEO Soldier, 2014b):

- Option 1: Do nothing. Make no decision at this time and continue the current situation of issuing soldiers UCP uniforms and equipment for all missions, except in Afghanistan where they would continue to get OEF CP uniforms and equipment.
- Option 2: Select OEF CP, accept the vendor's terms, and expand its use beyond Afghanistan to become the standard pattern of all Army uniforms and equipment.
- Option 3: Select ScorpionW2 and replace UCP uniforms and equipment over time when they wore out.
- Option 4: Select a digital transitional camouflage (DTC1) and replace UCP uniforms and equipment over time when they wore out.

Colonel Smith and his team considered these options the main courses of action for Army senior leaders to consider. The team debated the following decision criteria to apply to these options: performance, schedule, affordability/cost, legal risk, and the perspectives of key stakeholders such as soldiers, Congress, the Marine Corps, and the media.

Colonel Smith prepared for another challenging sets of meetings and did not like the thought of going back into the lion's den again with Army senior leaders in the Pentagon. This would be the third time he attempted to get a decision on camouflage for Army uniforms and equipment. However, he knew that the decision was of utmost importance for soldiers in combat. Effective camouflage increased soldier combat effectiveness and improved force protection—saving soldiers' lives in battle. Colonel Smith thought about the decision in terms of return of investment (ROI). From 2009 to 2014 (over six years), the Army spent less than $10 million in the research, development, and testing of camouflage patterns, but a camouflage change would affect the purchase of $5.2 billion of uniforms and equipment over the next 5–10 years (PM SPIE, PEO Soldier, 2013a, 2014c). Colonel Smith considered the research, development, and testing of camouflage patterns a wise investment for soldiers and for the American taxpayer.

Exhibit 2. Part II Case Study Discussion Questions

- Was $10 million spent over six years in the research, development, and testing of camouflaged uniforms a wise investment for the Army?
- Were the options considered by the Army appropriate? Were other viable options not considered?
- Was the source of funding (contingency funds or base budget funds) an important consideration? Why or why not?
- What were the affordability considerations for the Army in this decision?
- What were the important contractual and legal considerations in this decision?
- How should the Army compare the options and select the best path forward?

References

Hepfinger, L., Stewardson, C., Rock, K., Kramer, F. M., McIntosh, S., Patterson, J., Isherwood, K., Lesher, L., Rogers, G., & Nguyen, H. (2010). Soldier camouflage for Operation Enduring Freedom (OEF): Pattern-in-picture (PIP) technique for expedient human-in-the-loop camouflage assessment. Technical paper presented at the 27th Army Science Conference, Orlando, FL.

Lacey, D., & Rogers, G. (2014, June). Addendum to the final report for the Phase IV camouflage pattern testing, Stage II pattern testing for the Army combat uniform (transitional alternatives) (U.S. Army Aberdeen Test Center Report No. ATC-1150; Addendum). Aberdeen Proving Ground, MD: U.S. Army.

Mazz, J. (2014, August). Data analysis for the Army camouflage uniform improvement project: Phase IV, transitional pattern assessment (U.S. Army Materiel Systems Analysis Activity Technical Report No. TR-2014-39). Aberdeen Proving Ground, MD: U.S. Army.

Mazz, J., & Rowe, P. (2013, July). Data analysis for the Army camouflage uniform improvement project: Phase IV, Stage 2 (U.S. Army Materiel Systems Analysis Activity Technical Report No. TR-2013-39). Aberdeen Proving Ground, MD: U.S. Army.

Mortlock, R. (2016, October–December). Transfer MDA from top-level OSD and service officials and put it where it fits best: With the PEOs. Army AT&L, 120–124.

Natick Contracting Division, U.S. Army Contracting Command—APG. (2012a, January 9). Contract W911QY-12-C0033, awarded to Atlantic Diving Supply (ADS) Inc., Virginia Beach, VA.

Natick Contracting Division, U.S. Army Contracting Command—APG. (2012b, January 9). Contract W911QY-12-C0034, awarded to Brookwood Companies Inc., New York, NY.

Natick Contracting Division, U.S. Army Contracting Command—APG. (2012c, January 9). Contract W911QY-12-C0035, awarded to Crye Precision LLC, Brooklyn, NY.

Natick Contracting Division, U.S. Army Contracting Command—APG (2012d, January 9). Contract W911QY-12-C0036, awarded to Kryptek LEAF, Fairbanks, AK.

Office of the Secretary of the Army. (2009, September). Department of Army report to Congress on combat uniform camouflage. Washington, DC: Author.

Program Manager Soldier Protection and Individual Equipment (PM SPIE), Program Executive Office Soldier (PEO Soldier). (2013a, April 11). Army camouflage decision brief. PowerPoint presentation briefing prepared for Army Senior Leadership, Washington, DC.

Program Manager Soldier Protection and Individual Equipment (PM SPIE), Program Executive Office Soldier (PEO Soldier). (2013b, April 16). Army clothing update for SECARMY. PowerPoint presentation briefing prepared for Army Senior Leadership, Washington, DC.

Program Manager Soldier Protection and Individual Equipment (PM SPIE), Program Executive Office Soldier (PEO Soldier). (2013c, August 11). Army Phase IV camouflage update to SECARMY. PowerPoint presentation briefing prepared for Army Senior Leadership, Washington, DC.

Program Manager Soldier Protection and Individual Equipment (PM SPIE), Program Executive Office Soldier (PEO Soldier). (2013d, December 19). Army Phase IV camouflage update to the CSA. PowerPoint presentation briefing prepared for Army Senior Leadership, Washington, DC.

Program Manager Soldier Protection and Individual Equipment (PM SPIE), Program Executive Office Soldier (PEO Soldier). (2014a, January 29). Army Phase IV camouflage update to SECARMY. PowerPoint presentation briefing prepared for Army Senior Leadership, Washington, DC.

Program Manager Soldier Protection and Individual Equipment (PM SPIE), Program Executive Office Soldier (PEO Soldier). (2014b, May 2). Combat uniform camouflage update and decision brief. PowerPoint presentation briefing prepared for Army Senior Leadership, Washington, DC.

Program Manager Soldier Protection and Individual Equipment (PM SPIE), Program Executive Office Soldier (PEO Soldier). (2014c, July 15). Combat uniform camouflage effort [Memorandum]. Fort Belvoir, VA: Author.

Rogers, G., et al. (2013, September). Final report for phase IV camouflage stage II pattern testing for Army combat uniform (U.S. Army Aberdeen Test Center Report No. ATC-11250). Aberdeen Proving Ground, MD: U.S. Army.

Ryerson, C. C., et al. (2012, September). U.S. European Command (EUCOM) natural backgrounds and U.S. analogs (ERDC/CRREL M-12-1).

Ryerson, C. C., et al. (2013a, August). U.S. Pacific Command (PACOM) natural backgrounds and U.S. analogs (ERDC/CRREL M-13-1).

Ryerson, C. C., et al. (2013b, September). U.S. Northern Command (NORTHCOM) natural backgrounds and U.S. analogs (ERDC/CRREL M-13-2).

Ryerson, C. C., et al. (2013c, September). U.S. Central Command (CENTCOM) natural backgrounds and U.S. analogs (ERDC/CRREL M-13-3).

Ryerson, C. C., et al. (2013d, September). U.S. Africa Command (AFRICOM) natural backgrounds and U.S. analogs (ERDC/CRREL M-13-4).

Ryerson, C. C., et al. (2013e, October). U.S. Southern Command (SOUTHCOM) natural backgrounds and U.S. analogs (ERDC/CRREL M-13-5).

U.S. Army, Natick Soldier Research, Development, and Engineering Center (NSRDEC). (2004, December 15). Universal camouflage for the future force warrior. PowerPoint presentation briefing prepared for International Soldier Conference and Exhibition, Natick, MA.

U.S. Army, Natick Soldier Research, Development, and Engineering Center (NSRDEC). (2005, April). Development process of the universal camouflage for the future force warrior (Technical Report, Natick/TR-05/014L). Natick, MA: Author.

U.S. Army, Natick Soldier Research, Development, and Engineering Center (NSRDEC). (2009, June). Photosimulation camouflage detection test (Technical Report, Natick/TR-09/021L). Natick, MA: Author.

U.S. Army, Natick Soldier Research, Development, and Engineering Center (NSRDEC). (2012). Science supporting camouflage (Draft Technical Report, Natick/TR-12/022L). Natick, MA: Author.

U.S. Congress. (2013, December). Revised policy on ground combat and camouflage utility uniforms. In Fiscal Year 2014 National Defense Authorization Act (NDAA), Section 352, pp. 161–165.

U.S. House of Representatives. (2009, May). Making supplemental appropriations for the fiscal year ending September 30, 2009, and for other purposes (House Report 111-151). Washington, DC: Author.

Survive, But Not Thrive? The Constraining Influence of Government Funding on Technology Start-Ups

Capt Jason Rathje, USAF—is an active duty Air Force officer currently pursuing his PhD at Stanford's Management Science and Engineering Department. His research interests lie in the intersection of entrepreneurship, innovation, and national security. This includes an empirical evaluation of government funding on corporate strategy, supplemented by investigations into the knowledge economy and dual-use technology ventures. Prior to his time in graduate school, Capt Rathje served as both an Air Force and Joint Service acquisitions program manager and a flight test engineer. [jrathje@stanford.edu]

Abstract

This paper examines the potential constraining effects of funding from mission-oriented (e.g., NASA, DoD, DHS) public-funding agencies on the future growth of technology-based startups. Prior research on innovative, small-business government funding programs illuminates the beneficial nature of such public resources in overcoming resource limitations in launching new technology ventures. However, this research is based mainly on empirical analysis of non-constraining, grant-based relationships with science-oriented public-funding agencies and does not explicitly take the perspective of the entrepreneurial firm. I fill this gap by analyzing the potential limitations of government funding on technology start-up survival and growth. I argue that those government funding programs that constrain a start-up's strategic agility (i.e., limit opportunity discovery and exploitation) can have adverse long-term effects. By quantitatively examining over 27,000 technology start-ups, I find that such agility-constraining resources increase the likelihood of start-up survival, but limit growth. This paper, therefore, contributes to strategic management, entrepreneurship, and public policy literature.

Introduction

"In any given new technology, entrepreneurs could fail to identify any opportunities, or could identify the wrong opportunities, making an explanation for the discovery of opportunities an important part of the domain of entrepreneurship research" (Shane, 2000).

It is widely acknowledged that firms seeking to commercialize new technology ventures face significant resource constraints. Empirical evidence has shown that innovative companies suffer financing constraints for new technology ventures as conventional sources of for-profit capital (e.g., internal investment, VC, CVC) tend to under-invest in high-risk R&D (Howell, 2017; Lerner, 2012). In high-growth markets, where firms may experience fewer financing constraints, other resources become scarce. Acquiring technical talent, for example, can become a powerful constraint as ventures seek to scale in competitive labor markets (Kazanjian, 1988; Stern, Porter, & Furman, 2000). In combination, many firms fail in their attempts to bring new technologies to market.

To overcome resource constraints, it has long been the policy of nation-states with growth-focused economies to subsidize new technology ventures. While all firms face resource constraints in launching technology ventures, small firms feel the effects of these constraints the strongest (Gans & Stern, 2000). Small firms tend to suffer from an ability to appropriate social returns from their innovations and are therefore more likely to under-invest in new technology ventures (Anton & Yao, 1994). To counteract under-investment by small firms, governments have developed funding programs to subsidize innovation in small firms. These include such well-researched programs as the U.S. SBIR program (Howell, 2017; Link & Scott, 2010), the Chinese Innofund program (Guo, Guo, & Jiang, 2016; Wang, Li, & Furman, 2017), or the Swedish VINN NU program (Söderblom et al., 2015).

These subsidies tend to be particularly salient to resource-strapped technology start-ups (Kropp & Zolin, 2005). While small firms certainly face resource constraints, there are a large number of fixed costs for new firms that require additional resources. Thus, government funding programs that subsidize innovation in small firms tend to be overly prescribed by new firms. For example, in the U.S. SBIR program, 60% of all funding goes to firms under five years of age. Thus, technology start-ups are heavily represented in these early-stage R&D funding programs.

Research regarding the impact of small-business innovation funding policies has mainly found positive results. Primarily taking the view of the government, scholars have shown that such programs increased knowledge-spillovers leading to broader economic growth, overcame financial constraints in resource-strapped geographies, and increased the number of new technology ventures started from scientific endeavors as well as the number of commercial products introduced to market (Audretsch, 2003; Audretsch, Link, & Scott, 2002; Feldman & Kelley, 2006; Gans & Stern, 2000; Link & Scott, 2010). Of those scholars that have explicitly evaluated the impact of small-business innovation programs from the view of the firm, the majority have studied the effects of government funding on private R&D intensity (i.e., how much the firm spends internally on R&D), uncovering both complementary and substitutionary effects (Guerzoni & Raiteri, 2015; Wallsten, 2000). In general, these findings have found that small-business funding programs have had a positive impact on economic growth.

Interestingly, however, little research has explicitly investigated the impact of these programs on technology start-up performance. Recent research has indicated that scholars who study the effects of such government policies should expressly examine the nature of technology funding programs on entrepreneurial activity as opposed to grouping small businesses and start-ups under the same category (Hellmann & Thiele, 2017). Besides the large fixed costs of forming a new technology start-up, there exist significant differences in growth objectives and business models. What makes a small business successful, therefore, may not make a new firm successful. Given that prior research takes a macro-approach at evaluating the effect of these policies on economic and firm performance, there remains a gap in understanding how small-business innovation funding programs impact technology start-up performance.

This paper attempts to address this question by evaluating the potential negative influences of small-business funding programs on technology start-up growth. Specifically, I argue that while providing resources to technology start-ups increases the likelihood that they will survive, government-backed resources can impede growth by limiting a firm’s strategic agility. While resources remain critical for technology start-ups, that’s not all that necessary for a performant high-growth technology-start-up. Organizational research on entrepreneurial firms has illuminated how an entrepreneur’s cognitive and behavioral traits influence a new firm’s ability to discover and exploit optimal opportunities (Baron, 2007; Helfat & Peteraf, 2015). For example, scholars have shown that start-ups identify capabilities via cognitive frames that are generated through prior experiences (Baron, 2007; Baron & Ensley, 2006), engage in opportunities through rapid decision making governed by the firm’s standard operating procedures (Bakker & Shepherd, 2017; Eisenhardt, 1989; Ott, Eisenhardt, & Bingham, 2017) and are able to exploit opportunities via institutional bricolage (Baker & Nelson, 2005; Phillips & Tracey, 2007). In combination, new ventures with high strategic agility—the ability to recognize new opportunities, make important decisions about those opportunities quickly, and re-deploy institutional resources to exploit those opportunities—are more likely to be successful. Thus, engaging with resources which constrain strategic agility may weaken firm performance.

To test these theories, I analyze a matched sample of 27,730 dual-use technology start-ups. Dual-use technology ventures are a particularly appropriate research setting as they have the option to receive funding from both private sources of capital and mission-funding agencies. Many technology ventures are considered dual-use (cybersecurity, artificial intelligence, etc.), thus making it a particularly important part of the high-technology economy (Lin, 2016). Funding from a mission-funding agency (e.g., militaries, space agencies, homeland security agencies) provides a particularly salient example of an agility constraining opportunities, as mission funding agencies often have unique, monopsony needs, restrictive contractually-based mechanisms, and pre-set resource allocation rules that limit a firm's ability to discover and exploit opportunities. In combination, dual-use technology start-ups have multiple initial resource opportunities and therefore can select into potentially constraining ones.

To test the impact of these programs, I employ a quasi-experimental design through a robust matching, cox-proportional hazard, and differences-in-differences approaches. Specifically, I assess the impact of the DoD's SBIR program on technology start-up survival and growth (number of employees and revenue, logged). By collecting quantitative and qualitative evidence, I find that the DoD SBIR program provides much-needed sources of revenue for firms and that firms receiving SBIR contracts experience more extended survival rates. Interestingly, however, I find that firms who receive SBIR contracts from the DoD establish patterns of behavior that limit strategic agility. Quantitatively, I show that for SBIR-start-ups, post-award growth is slower, as revenue is net-negative compared to a comparable set of industry peers.

I make two contributions. First, I contribute to strategic management by introducing the concept of an agility-constraining opportunity. While prior research has focused on how firms become more agile by discovering and exploiting opportunities, this paper argues that discovering and exploiting an agility-constraining opportunity can have long-lasting adverse effects where competitors have multiple resource paths to pursue. Second, I contribute to policy research by detailing the conditions under which firms might be more or less successful when partnering with the government. Specifically, I show that the impacts of government funding for new ventures are distinct from more traditional small businesses. By showing how small-business funding programs can be determinantal for growth in new firms, I argue for new policy which takes entrepreneurial growth goals and business models into consideration.

Research Setting

I explore this question by investigating the impact of the U.S. Department of Defense (DoD) Small Business Innovative Research (SBIR) program on new venture survival and growth. The SBIR program was instantiated to specifically counter-act underinvestment from small businesses in new technology ventures (Audretsch, 2003; Audretsch, Weigand, & Weigand, 2002). Funding for the SBIR program is significant, with the total spending breaching $2.5 billion in 2017. Subsequently, the SBIR program remains one of the most well-researched small business programs and is a model for both OECD and non-OECD countries seeking to develop their innovation funding programs (Wang et al., 2017).

Although prior research often investigates the U.S. SBIR program in its entirety, there is significant heterogeneity within the program itself. The SBIR program is funded directly by individual government funding agencies, such as the Department of Energy (DoE), National Science Foundation (NSF), or the National Air and Space Administration

(NASA). Specifically, each funding agencies allocates 3.2% of their annual extra-mural R&D budget (i.e., the part of the yearly budget dedicated toward funding R&D external to the organization) towards the SBIR program. Accordingly, each funding agency is allowed to decide how to allocate those funds, leading to significant heterogeneity in policy implementation. Variation in funding strategy includes differences in which technology sectors to fund (i.e., energy vs. space), the maturity of technology required prior to funding (i.e., basic through applied research), and the nature of the interaction between government agency and funded firm (i.e., grant-based or contractually-based relationships).

To best research how government funding might constrain technology start-up strategic agility, the U.S. DoD SBIR program presents a particularly salient example. Prior research has focused primarily on science-oriented funding agencies funding new technology ventures through grant-based relationships (Bruce, de Figueiredo, & Silverman, 2018; Pahnke, Katila, & Eisenhardt, 2015). The DoD is a mission-oriented funding agency which caters to public-sector demands through contract-based relationships, which creates two significant differences from this prior work. First, while previous research generally studies the impacts of public funding programs administered by science-oriented funding agencies who fund firms to introduce new technology ventures to the private-sector market, mission-oriented funding agencies fund firms to introduce new technologies to public and private-sector markets. The DoD, for example, controls the market for military technologies and therefore invests in technology ventures which have the potential for commercial application internal to the military (Dasgupta & David, 1994; Mowery, 2009). As a result, DoD SBIR funding heavily incentivizes firms to develop products or services to meet military demands.

Second, while prior research has generally studied the impact of funding programs which allocate funds through unrestrictive grant-based relationships, the DoD funds technology ventures through more restrictive, contractually-based relationships (Congress, 1977; Flammer, 2018). In grant-based relationships, firms may adapt or alter their R&D activity as more knowledge is gleaned in the course of the R&D activity. In contrast, any change in R&D activity in a contract-based relationship requires a re-negotiation of the contract itself. As a result, DoD SBIR funding incentivizes firms not to adjust R&D activity. In combination, the public-sector demands of the DoD and the generally restrictive nature of contractually-based relationships make the U.S. DoD SBIR program a particularly useful context from which to measure the impact of small-business innovative funding programs on technology start-up performance.

Theory Building and Hypotheses

Research at the intersection of entrepreneurial strategy and technology start-up performance highlights three important firm-based performance outcomes: firm survival, firm growth, and innovations produced (normally assessed by patents or product introductions). Research intersecting technology start-ups and government funding has primarily evaluated the later and has generally found that government R&D funding dedicated to innovation results in both more technologies invented and products introduced (Audretsch, 2003). For example, the only two studies that specifically address the impact of mission organizations—one on NASA and the other on the DoD—use survey and case-based evidence to show that SBIR-contract receiving companies report both an increase in the number of new technology ventures embarked and number of commercial products successfully introduced to market (Archibald & Finifter, 2003; Audretsch, Link, et al., 2002). Therefore, this paper focuses solely on the impact of the U.S. SBIR funding program on technology start-up survival and growth.

Government Funding and Firm Survival

Entrepreneurial cannon on growth-focused technology start-ups has long emphasized the importance of acquiring critical resources quickly. These include access to capital, access to capable technical talent, and both technical and social legitimacy (Armanios et al., 2017a; Eberhart, 2017; Hsu, Roberts, & Eesley, 2007; Lerner, 1999). Finding and employing capital is vital given that technology start-ups incur significant costs before generating revenue. Finding and hiring technical talent is important given limited technical labor supply and the need to scale effectively and quickly. Gaining both technical legitimacy and social legitimacy is important to generate ties with resource providers (e.g., suppliers, customers, strategic alliances). In sum, for technology start-ups to survive, they must quickly acquire critical resources.

Government funding can be particularly useful in providing such resources. First, government subsidy programs provide direct, non-dilutive capital to firms. The SBIR program offers, on average, up to $225,000 for an early stage contract. While this amount of funding might not be significant for larger, more established firms, it is precious for early-stage companies. In comparison, the median angel investment round, which would be the comparable private capital funding mechanism, is ~$285,000. Furthermore, while the median angel investor charges ~8% equity for that initial investment, the SBIR program takes no equity stake (Knauss, Edwards, & Williams, 2017). Government funding is therefore particularly attractive to technology start-ups.

Second, government funding provides access to technical experts. Access to government researchers is a critical part of government funding programs that invest in new technology ventures (Sauermann & Stephan, 2012). Across all U.S. funding agencies, for example, SBIR projects are administered by advanced-degree holding researchers who work directly with the funded companies (SBA, 2014). These government researchers spend significant time with the funded company to help the firm meet its funded R&D goals (Pahnke et al., 2015). The government also indirectly incentivizes interaction with non-government backed technical experts as displayed in program selection biases. For example, Feldman and Kelley (2006) find that firms who partner with research institutions experience higher likelihoods of receiving government funding. Thus, technical talent is a crucial resource provided by government funding partnerships.

Lastly, government funding supports technical and social legitimacy via certification and access to a stabilizing set of government ties. Given their resident technical expertise, partnering with a government organization is interpreted as a certifying stamp of technical legitimacy (Armanios et al., 2017b; Eesley, Li, & Yang, 2016). Studying 151 Chinese entrepreneurs who entered a funding partnership with the Chinese government, Armanios et al. (2017) showed that while the entrepreneurs benefited from the resident technical expertise (skill adequacy), those entrepreneurs who were relative unknowns in the social context benefited significantly more from the certification received by participating in the program. Explicitly, the technical quality of the entrepreneur is signaled by the government's certification of the firm. Similar research has been done investigating firms who partnered with the government in Finland (Autio & Rannikko, 2016) and Spain (Busom, 2000).

Government partnerships also provide social legitimacy by enforcing a stabilizing series of political ties between government funding agency and firms. Research has illuminated that political ties generate important social legitimacy for firms dealing with uncertain environments (Hiatt, Carlos, & Sine, 2017; Hillman, Zardkoohi, & Bierman, 1990; Wang & Qian, 2011). For example, researching 282 airline ventures in 10 South American countries, Hiatt et al. (2017) found that those airlines which had political ties with the military were more likely to survive in times of social unrest. Thus, the very nature of receiving a government contract can increase a technology start-up's technical and social legitimacy.

Given access to unique, technical, and high-capital resources, along with sources of legitimacy from technical certification and political ties, government funding provides a unique set of resources for technology start-ups. I argue that, in combination, these positive externalities of government funding make it much more likely for firms who receive government funding to survive relative to those firms who do not engage in such partnerships. This leads me to my first hypothesis:

H1: Technology start-ups who receive government funding are more likely to survive than similar firms who do not.

Government Funding and Firm Growth

Entrepreneurial cannon has also established that firms grow by rapidly discovering and exploiting novel opportunities (Eckhardt & Shane, 2003; Hitt et al., 2001; Ireland, 2007; Shane & Venkataraman, 2000). Prior work in strategic management has introduced the concept of strategic agility—that is, the ability rapidly identify and engage in profitable opportunities—as a core trait of successful entrepreneurial firms (Doz & Kosonen, 2010; Ryu, Kwon, & Park, 2018). This can best be broken down into three distinct parts: identifying capabilities by employing multiple and heterogeneous cognitive frames, rapidly experimenting, evaluating, and selecting opportunities by applying reliable and repeatable standard operating procedures, and exploiting opportunities via bricolage (reconfiguring and deploying resources in novel ways). Technology start-ups that can effectively engage all three activities exhibit high strategic agility, allowing them to discover and exploit valuable opportunities which result in firm growth.

When government funding constrains strategic agility, therefore, it may have a limiting effect on future growth. Given that the U.S. DoD SBIR program has unique, public-sector demands and employs more restrictive, contractually-based relationships, firms who receive DoD SBIR contracts may experience impediments to growth. Specifically, I argue such funding programs impose two unique impediments on technology start-ups: *institutional impediments*, which limit opportunity identification, and *structural impediments*, which limit opportunity evaluation speed and resource bricolage, respectively. For example, by encouraging technical performance (a unique, public-sector demand) over-commercialization, mission-funding agencies incentivize firms to seek professional opportunities for new technology ventures instead of growth opportunities for which to introduce new commercial products (Eesley, 2016; Sauermann & Stephan, 2012). In turn, the potential impediments caused by agility-constraining government funding may limit growth.

Institutional Impediments

Institutional impediments are initiated via differences in institutionalized norms and behaviors between mission-oriented government funding sources and that of technology start-ups. Norms of mission-oriented funding agencies, derived from the institution of the state, have been characterized by a focus on new technology ventures to support unique, mission-focused demands (Branscomb, 1993; Prendergast, 2002; Thornton, Ocasio, & Lounsbury, 2012). For example, the primary objective of the U.S. SBIR program is to "fund innovative new technology ventures." Conversely, norms of technology start-ups, derived from the institution of the corporation, have been characterized by a focus on resource acquisition, market-driven research, and controlling access to intellectual property (Liebeskind, 1996). I argue that by incentivizing technology start-ups to follow mission-oriented funding agency norms instead of technology start-up norms, government funding sources limit the ability for start-ups to identify growth opportunities.

Scholars have shown that new firms often adopt the norms and behaviors of their critical resource providers. For example, Grégoire et al. (2010) showed that how start-ups recognize opportunities is driven by prior experiences and present network structure. Gulati & Higgins (2003) find a firm’s future experiences are limited to those made available by early-influencing partners, re-enforcing initial opportunity recognition behavior. Thus, for start-ups whose only experiences are constrained to interactions with mission-oriented funding agencies, opportunity recognition will be driven by a set of norms and behaviors that prioritizes new-venture formation over existing-venture growth.

Indeed, interviews with entrepreneurs highlight some such effects. For example, the founder of one company who received multiple U.S. DoD SBIR awards pined over his failure to recognize commercial-funding opportunities. He stated,

> One of my regrets of course having wizened up after this [company failure due to slow growth] and maybe this is the lesson that is we should have gotten commercial funding earlier. … It wasn’t a question of not wanting to give away a part of the company or equity. I think we were just a little risk averse and weren’t sure, and I don't know why. Why we were risk averse to the idea of getting any commercial funding and things of that nature. So, in retrospect I think, had we 10 years ago gone and gotten some commercial funding, things would've been very different.

He attributed his firm’s ultimate demise to not recognizing commercial opportunities, prioritizing winning multiple SBIR awards instead of pursuing alternative sources of revenue or investment.

It, therefore, stands to reason that opportunities driven by the government, as opposed to commercial markets, become more salient as the ties with the government become stronger. While capitalizing on such opportunities may be beneficial for capturing the future government market, they may limit the opportunity to identify growth-focused opportunities.

Structural Impediments

Structural impediments are driven by the contractual nature of relationships between mission-oriented government funding agencies and their partnered firms. *Contracts* are a “binding agreement between a buyer (government) and seller (firm) to provide goods in return for compensation” (Congress, 1977). Unlike grants, when the public-funding sponsor has limited insight into R&D activity in the private firm, in contracts the public partner has a significant say, and imparts strategic direction, on the firm’s R&D activity. They are often executed on behalf of public, mission-oriented funding agencies as these agencies cater to specific public-markets with unique public-sector demands (David & Hall, 2000). For example, while both mission and non-mission funding agencies execute SBIR programs, SBIR-based public-private R&D relationships with the NIH (non-mission) collaborate use grants, while relationships with the DoD (mission) use contracts. Thus, those start-ups who engage with the U.S. DoD SBIR program do with through more intensive, contract-based relationships.

Contracts impose two structural impediments which constrain strategic agility. First, government program managers enforce mission-oriented demands on firms. On one hand, mission-oriented demands result in highly organized and formalized approaches to R&D activity. On the other, it enforces a large time cost on behalf of the developing firm, which limits the firm's ability to rapidly experiment with emerging opportunities. For example, contracts require statements of work, which describe—to specific technical detail—the proposed R&D path as well as the ultimate contract deliverables. This requires significant work on behalf of the entrepreneur. For example, a private investor who invested in 10 SBIR-receiving companies stated,

> There was a fairly involved process of actually negotiating the deliverables and the timelines and whatever went into an agreement that was crafted. I'm not sure if every single one of the applications needed it, but I've heard back from some of them that this took a bit of doing, that this was a fairly long process, because some of the funds were dispersed in transfers and they had to accomplish certain things, and so they had to put in place various goals and deliverables and things like that, so that took a bit of doing.

Thus, engaging in contracts can impart significant time costs to the partnered firm.

Second, if the technology start-up wishes to alter its development path, it requires contractual revisions. The Federal Acquisition Regulation, the U.S. federal law which governs contract usage, clarifies that contract change agreements are required when the firm or government funding agency wishes to change a Statement of Work. An investor discussed how that could be damaging to start-ups who are continually adapting as new information becomes available in the R&D process. He stated, "If, down the road, they [the start-up] suddenly had to change their funding allocation or something changed that they didn't anticipate, and this renegotiation of the spending and the budgetary items took a little bit of time." In turn, contracts make it difficult to pivot R&D as new information emerges.

In combination, structural impediments constrain the ability to evaluate rapidly and deploy resources against, new opportunities. Lengthy contract negotiations limit rapid decision making, while contractual revisions restrict the ability to quickly re-deploy resources. In sum, although government-funding may increase firm survival, I argue that funding from mission-oriented funding agencies can impede growth. Specifically, institutional and structural impediments limit the ability of firms to recognize and rapidly exploit novel opportunities. Therefore, my second hypothesis is as follows:

H2: Technology start-ups which receive government funding from mission-oriented funding agencies are associated with slower growth than firms who do not.

Methods

Data

I analyze the associations between the U.S. DoD SBIR program and technology start-up performance over 15 years from 1997–2012. My sample comprises specifically of *dual-use technology firms* (referred to as "dual-use firms" from here on out). Dual-use firms are defined as technology firms who can sell products to the public or private sector. These firms comprise significantly large industries, such as aerospace, cybersecurity, and IT. I choose to analyze dual-use as they have multiple types of investors and a large variety of potential go-to-market strategies. They therefore represent a set of firms that face the question of if, and with whom, to receive funding from.

I begin my sample by collecting the full population of new ventures who received funding from the U.S. Department of Defense (DoD) Small Business Innovative Research (SBIR) program from 1997–2012. Out of the total DoD SBIR awarded firms in between these years, more than 60% of the companies who received SBIR contracts were new ventures. A new venture qualifies any firm less than five years of age at the time of winning their first SBIR contract.

Next, I collect data on all firms in the sample dating back to 1994, the year the government mandated SBIR contract-receiving companies register in Dun and Bradstreet, thus providing the best starting point for data collection. Although the oldest firm in the sample is founded in 1997, beginning data collection in 1994 allows controlling for financial capabilities up-to three years before receiving an SBIR award. Although my sample ended in 2012, I continue data collection through 2015 or until the firm declares bankruptcy, or is acquired. This allows for additional outcome analysis. One resulting strength of my data set is that it contains the entire population of new, DoD SBIR-funding receiving firms during this time. There are 1,965 total firms in my data set, all founded between 1997 and 2012.

To develop a sample of dual-use firms, I next sample Dun and Bradstreet for firms with a similar founding year and SIC. Since firms register in Dun and Bradstreet when they seek a credit rating, the resulting data set is particularly complete (Eesley & Roberts, 2012). Specifically, I query every U.S. firm in Dun and Bradstreet founded between 1997 and 2012 which shares at least one 4-digit Standard Industrial Code (SIC) in common with the SBIR receiving firms. Comparable firms are limited to the United States as all SBIR companies must be at least 51% owned in the United States. Four-digit SIC is a useful measure of a firm's industry at the level of product offerings. For example, the 2-digit code 36 classifies "Electronic and Other Equipment" companies, while adding two more digits to get to the 4-digit code of "3672" classifies the firm as producing "Printed Circuit Boards." Combining these data sets, I compiled a total sample of 358,535 firms.

My primary data set is was collected from the SBIR database (SBIR.gov) and Dun and Bradstreet. To measure venture-backed funding partnerships and pertinent, annual firm performance data, I utilized Thompson One and PitchBook. Where there were discrepancies, I turned to other data sources for clarification, include CapitalIQ, Crunch Base, and Data Fox.

Measures

Dependent Measures

The first hypothesis measures the likelihood of firm survival. Given the lack of commonly-available standard performance information for newly formed private-ventures, firm survival is an important and commonly used metric of new-venture performance (Chatterji, 2009; Klepper, 2002; Paik, 2014). This is captured in two variables, *exited* and *exit-date*. Exited is measured by a binary variable of whether a firm goes out of business, 1 if it goes out of existence and 0 if it still exists. This does not include acquisition or IPO, as those exit strategies may qualify as still "surviving," although in a different format. *Exit-date* is qualified as the year in which the firm goes out of business. In combination, both variables are used to analyze the first hypothesis.

For robustness, I also evaluate *Acquired,* as acquisition represents a potentially positive outcome for young firms and therefore a distinctly alternative exit strategy. Given the SBIR program's data rights clauses, and that those rights are transferable through acquisition, SBIR companies who developed unique and innovative technologies are likely to become acquisition targets for larger firms. *Acquired* is measured by a binary variable of whether a firm was acquired, 1 if acquired and 0 if not.

The primary aim of hypothesis two is to measure the influence of funding on entrepreneurial growth. I define growth in two dimensions, *Log Revenue* and *Log Employees*. *Log Revenue* is used as it is strategy invariant, as the majority of start-ups seek revenue regardless of growth, IPO, or acquisition strategy (Eesley & Roberts, 2012). Specifically, I calculate log revenue as the log of revenue in each firm-year of operation. As employees indicate growth goals, I also include *log employees.* Log employees are calculated as the log of employees in each firm-year of operation.

Independent Measures

I operationalized my main explanatory variable of interest with *SBIR-awardee.* I measured whether a firm received government funding with an *SBIR-awardee* binary variable coded as 1 if the firm received an SBIR contract and 0 otherwise. Multiple awardee recipients were recorded in the *Number of SBIR awards* variable.

Controls

Given the different measures of performance, the following controls are either recorded at the founding, before award, or per firm-year, depending on the needs of the model. For assessing survival rates, our variables do not change in time. For evaluating growth, some variables—where required—are measured as lagged by one year.

I measured whether the firm received *venture-funding* with a binary variable coded as 1 if the firm received VC investment and 0 otherwise. As prominent VCs may be more likely to influence innovation, I also measured relationship to high-status VCs for sensitivity analysis. VC's eigenvector centrality in venture capital syndication networks was included to control for ranking, and the top 30 VCs were coded with a 1 in the binary variable *Top-tier VC.*

Since older firms are correlated with higher revenues and more employees, I control for *firm age.* Firm age is the difference between the founding year as reported in the Dun and Bradstreet database and current year. As *the industry* is an essential discriminant in performance, I also control for the 4-digit *SIC*. I build on prior literature that uses this level of detail to describe industry effects (Zajac, 1988). I also control for the location with *state.* SBIR program restricts funding companies to which U.S. citizens own 51% of the firm. Therefore, all of the firms in our data set are U.S. based. State is a dummy variable across all 50 states.

I control for firm technical resources with firm *patents.* I.P. owned and appropriated before SBIR or Venture award may affect both the likelihood of firms receiving an award and entering into a contractual arrangement. Patents are recorded as the total number of patents awarded in a given firm-year.

I also include a standard control for *founding team size*. Larger founding teams are known to be correlated with higher performance outcomes. It is well acknowledged that the range of an entrepreneur's ex-ante functional expertise and experience will influence organizational decisions, and therefore the greater the team size, the higher the functional collective knowledge (Beckman & Burton, 2008; Gompers, 2005). I measure team size by the number of founders (Pahnke et al., 2015). Founding team size is recorded as the total number of employees listed on Dun and Bradstreet at the time of founding (Eisenhardt & Schoonhoven, 1990).

I also control for *Woman* and *Minority*-owned businesses. The U.S. Small Business Association, which oversees the SBIR program, gives special attention to, and incentivizes participation from, woman and minority-owned businesses (Bramble, 2015; SBA, 2014). As a woman and minority businesses may be therefore more likely to apply to SBIR, they represent a necessary control. Woman and minority are binary variables recorded as 1 if at least 51% owned by one or more women or minorities, respectively.[1]

Finally, I control for *temporal effects* that might be correlated with performance outcomes given macroeconomic conditions beyond our control. Temporal effects are measured with yearly dummy variables from 1994 to 2015, strictly for growth models.

Methods

I take a quasi-experimental approach towards assessing our hypotheses. This involves a process that controls for *selection* through matching methods, by applying both strict sub-sampling and coarsened-exact-matching, and *treatment*, by applying cox-proportional hazard model and differences-in-differences methods

Matching

The goal of the matching method is to generate matched sets of control-treatment firms that are as close as possible so they can be used to estimate the counterfactual in ways that are relevant for the outcome (Shadish, Cook, & Campbell, 2002). Given the large sample size available, I employ strict sub-sampling (Stuart, 2010). Strict sub-sampling matches firms exactly on matching covariates, resulting in K-1 matches (control to treatment). Given previous research that has applied similar methods, I matched firms on geographical location, founding year, and SIC (Goldstein & Narayanamurti, 2018; Pahnke et al., 2015). Altogether, I create matched sets of firms that receive SBIR. For the primary sample, this reduced total firms in the analysis to 27,730 firms, 1,414 received at least one SBIR contract.

Cox Proportional Hazard

To test the survival rate of firms, I build on previous literature examining firm longevity by employing the proportional hazards modeling as described by Cox (Audretsch & Mahmood, 1995; Mata & Portual, 1994; Suarez & Ulterback, 1995). This method uses a logarithmic transformation of a hazard of failure as the outcome variable. As firms experience a higher likelihood of failures, their hazard rate shifts upwards. The hazard model is

$$\ln\ h(t) = \ln h_0(t) + X\beta,$$

where $h_0(t)$ is the baseline hazard function, X is a vector of covariates, and β is a vector of the coefficients. The resultant prediction of the hazard function shows a value greater than 0.5 if a firm is likely to exit relative to its control group. A negative value implies that a firm is more likely to survive.

Difference-in-Differences

I use a differences-in-differences approach to asses longitudinal performance. Estimating treatment effects by constructing a matched control group and analyzing panel

[1] The definition of minority is supplied by the U.S. Small Business Association and is publicly available. These include minority groups which are presumed to be socially and economically disadvantaged, such as African Americans, Hispanic Americans, Native Americans, Alaska Native Corporations, Indian Tribes, Native Hawaiian Organizations, Community Development Corporations, Asian Pacific Americans, and Subcontinent Asian Americans.

data using a difference-in-differences approach has shown to be a robust approach to evaluating policy treatments, such as government funding (Short & Toffel, 2010). This method yields separate estimates for selection and treatment effects and allows a comparison of treatments over time, which is essential when measuring changes in the rate of growth post-treatment. H1 is measured with Cox-proportional hazard model, while H2 is measured with the differences in differences approach.

Results

The central results of the paper are shown in Tables 2 and 3. Model 2, Table 2 represents the impact of SBIR funding on start-up survival. Models 2 and 4, Table 3, represent the associations between government funding and start-up growth. Figures 1 and 2 summarize these results by showing differences in firm performance pre and post-award. Table 1 presents covariate descriptive statistics, post-match.

Table 1. Means, Standard Deviations, and Correlations

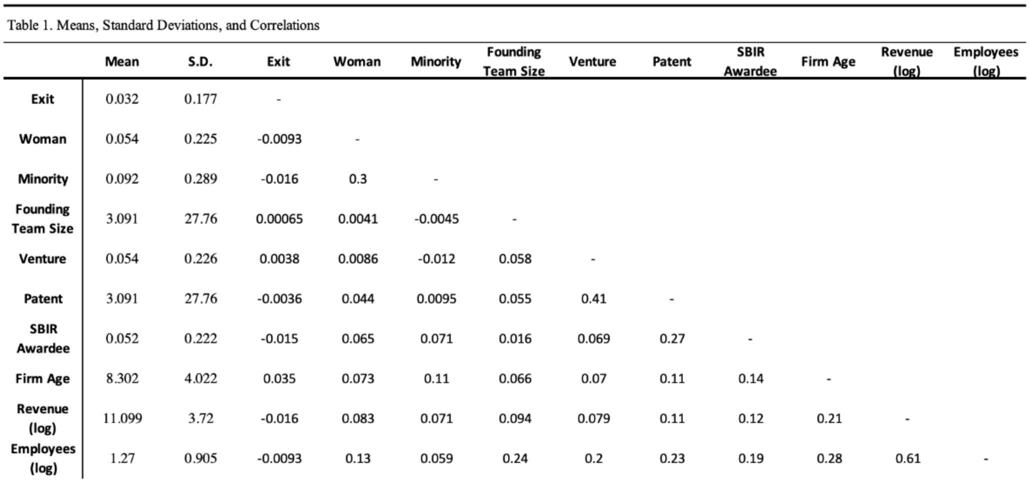


Table 1. Means, Standard Deviations, and Correlations

	Mean	S.D.	Exit	Woman	Minority	Founding Team Size	Venture	Patent	SBIR Awardee	Firm Age	Revenue (log)	Employees (log)
Exit	0.032	0.177	-									
Woman	0.054	0.225	-0.0093	-								
Minority	0.092	0.289	-0.016	0.3	-							
Founding Team Size	3.091	27.76	0.00065	0.0041	-0.0045	-						
Venture	0.054	0.226	0.0038	0.0086	-0.012	0.058	-					
Patent	3.091	27.76	-0.0036	0.044	0.0095	0.055	0.41	-				
SBIR Awardee	0.052	0.222	-0.015	0.065	0.071	0.016	0.069	0.27	-			
Firm Age	8.302	4.022	0.035	0.073	0.11	0.066	0.07	0.11	0.14	-		
Revenue (log)	11.099	3.72	-0.016	0.083	0.071	0.094	0.079	0.11	0.12	0.21	-	
Employees (log)	1.27	0.905	-0.0093	0.13	0.059	0.24	0.2	0.23	0.19	0.28	0.61	-

Table 2 represents the cox-proportional hazard model for firm survival. I find evidence to support H1. Model 2 shows that SBIR awards have a significant and negative impact on firm death, thus leading to higher survival rates. Specifically, these results indicate that firms which receive a contract early in their existence have a 60% greater chance of survival as compared to those similar firms which do not win a government contract.

Table 2. Exit: Cox Proportional Hazard Model

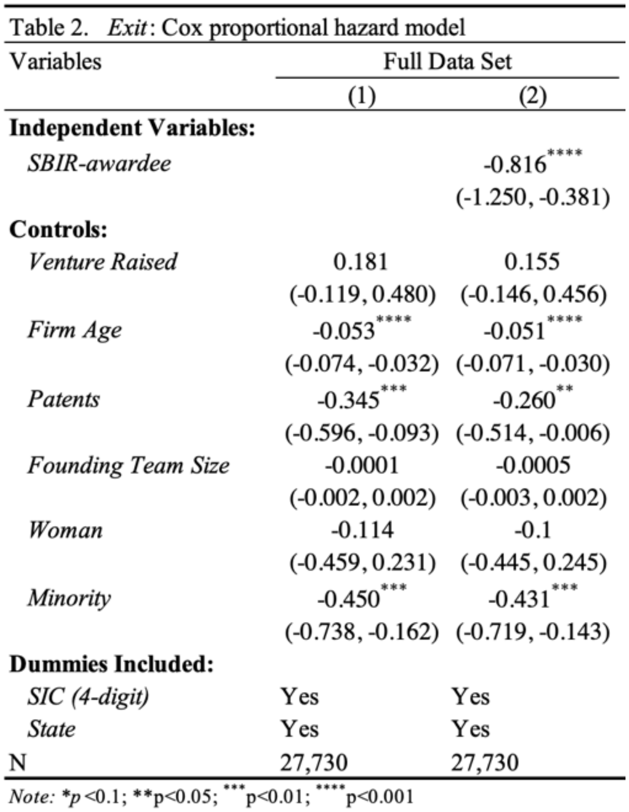


Table 2. *Exit*: Cox proportional hazard model

Variables	Full Data Set	
	(1)	(2)
Independent Variables:		
SBIR-awardee		-0.816^{****}
		(-1.250, -0.381)
Controls:		
Venture Raised	0.181	0.155
	(-0.119, 0.480)	(-0.146, 0.456)
Firm Age	-0.053^{****}	-0.051^{****}
	(-0.074, -0.032)	(-0.071, -0.030)
Patents	-0.345^{***}	-0.260^{**}
	(-0.596, -0.093)	(-0.514, -0.006)
Founding Team Size	-0.0001	-0.0005
	(-0.002, 0.002)	(-0.003, 0.002)
Woman	-0.114	-0.1
	(-0.459, 0.231)	(-0.445, 0.245)
Minority	-0.450^{***}	-0.431^{***}
	(-0.738, -0.162)	(-0.719, -0.143)
Dummies Included:		
SIC (4-digit)	Yes	Yes
State	Yes	Yes
N	27,730	27,730

Note: **p* <0.1; **p<0.05; ***p<0.01; ****p<0.001

Table 3 represents the differences in differences models for firm growth. I find partial evidence for H2. First, Models 2 and 4 (SBIR-awardee variable) indicate that SBIR contracts are awarded to higher performing firms. This indicates a significant and positive selection effect for SBIR awards, consistent with earlier research. Second, Model 2 (SBIR-awardee x After treatment variable) indicates weaker revenue growth post-award, while Model 4 indicates stronger employee growth. Specifically, Model 4 suggests that contract-receiving firms experience ~10% greater employee growth post-SBIR award, while Model 2 shows that those same firms experience a 70% decrease in revenue. I return to these intriguing findings in the conclusion.

Table 3. Diff-in-Diff

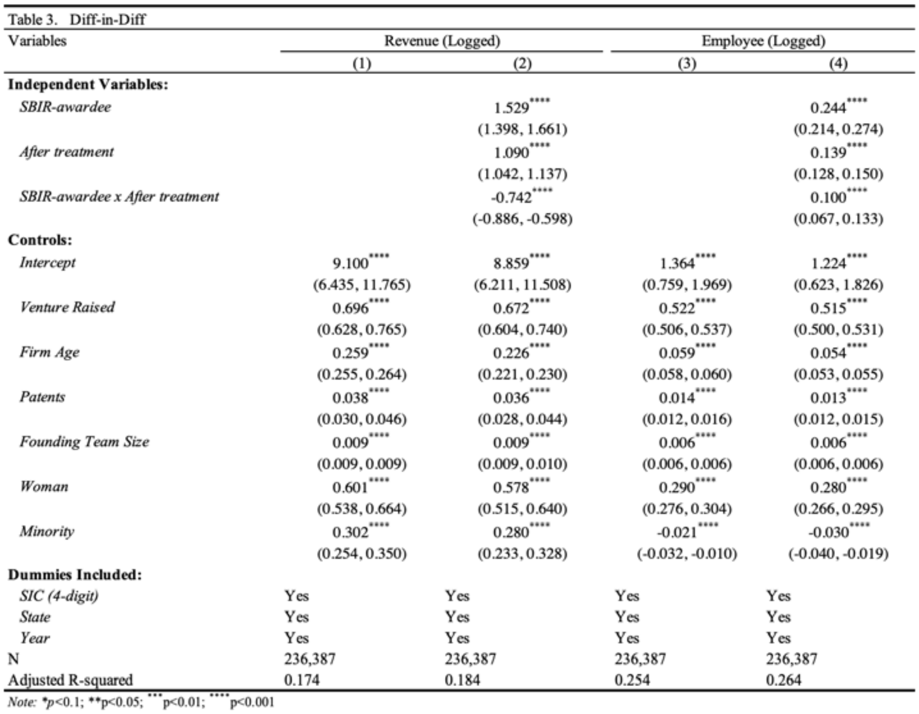


Table 3. Diff-in-Diff

Variables	Revenue (Logged)		Employee (Logged)	
	(1)	(2)	(3)	(4)
Independent Variables:				
SBIR-awardee		1.529****		0.244****
		(1.398, 1.661)		(0.214, 0.274)
After treatment		1.090****		0.139****
		(1.042, 1.137)		(0.128, 0.150)
SBIR-awardee x After treatment		-0.742****		0.100****
		(-0.886, -0.598)		(0.067, 0.133)
Controls:				
Intercept	9.100****	8.859****	1.364****	1.224****
	(6.435, 11.765)	(6.211, 11.508)	(0.759, 1.969)	(0.623, 1.826)
Venture Raised	0.696****	0.672****	0.522****	0.515****
	(0.628, 0.765)	(0.604, 0.740)	(0.506, 0.537)	(0.500, 0.531)
Firm Age	0.259****	0.226****	0.059****	0.054****
	(0.255, 0.264)	(0.221, 0.230)	(0.058, 0.060)	(0.053, 0.055)
Patents	0.038****	0.036****	0.014****	0.013****
	(0.030, 0.046)	(0.028, 0.044)	(0.012, 0.016)	(0.012, 0.015)
Founding Team Size	0.009****	0.009****	0.006****	0.006****
	(0.009, 0.009)	(0.009, 0.010)	(0.006, 0.006)	(0.006, 0.006)
Woman	0.601****	0.578****	0.290****	0.280****
	(0.538, 0.664)	(0.515, 0.640)	(0.276, 0.304)	(0.266, 0.295)
Minority	0.302****	0.280****	-0.021****	-0.030****
	(0.254, 0.350)	(0.233, 0.328)	(-0.032, -0.010)	(-0.040, -0.019)
Dummies Included:				
SIC (4-digit)	Yes	Yes	Yes	Yes
State	Yes	Yes	Yes	Yes
Year	Yes	Yes	Yes	Yes
N	236,387	236,387	236,387	236,387
Adjusted R-squared	0.174	0.184	0.254	0.264

Note: *p<0.1; **p<0.05; ***p<0.01; ****p<0.001

Figure 1 represents the differences-in-differences graphs. The graph on the left indicates that firms who receive SBIR awards have greater revenue before award, but firms who do not win SBIR awards experience stronger growth post award. As successful firms experience their initial sources of revenue during this period (between 2 and 4 years of age), this result is consistent with existing empirical research. The graph on the right indicates that firms who receive SBIR awards do experience stronger employee growth post award.

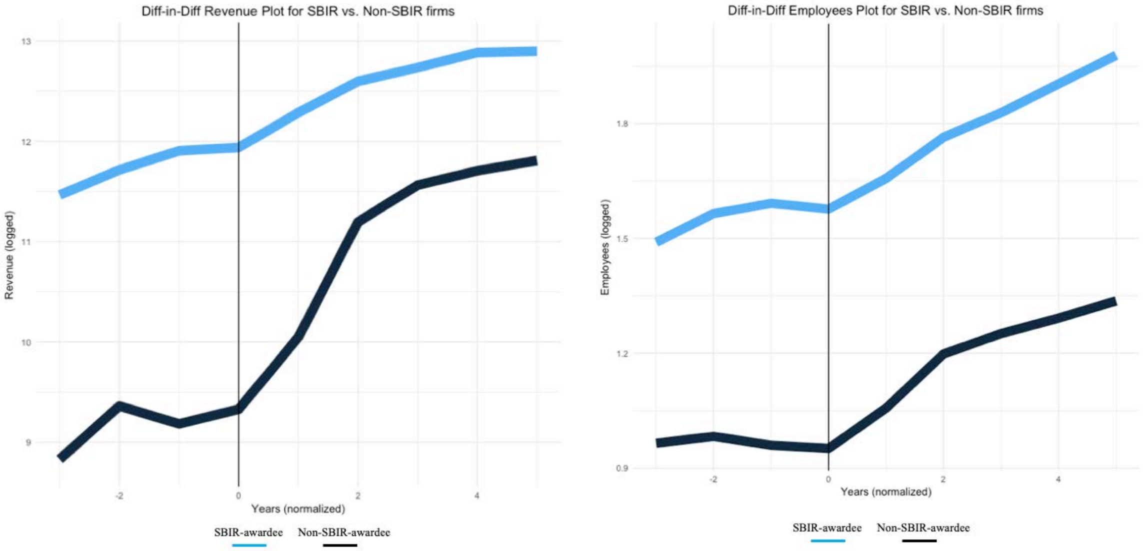


Figure 1. **-Diff-in-Diff Plots for Revenue (Left) and Employees (Right)**

Note. Plots are interpreted by differences in growth post award. Non-SBIR receiving firms experience rapid revenue growth post award, while SBIR receiving firms experience greater employee growth post award.

Also of interest are a few covariates. Notably, the countervailing effects of venture financing indicate some intriguing results. Table 2 shows that venture raised has a positive, if not a significant impact, on firm death. While potentially counter-intuitive, this is mostly consistent with recent empirical research which indicates that venture capital accelerates both firm growth and firm death. Given that government funding protects against some of the volatility inherent in VC-backed growth strategies, we would expect to find differentiated results between government funding and venture funding. Table 3 shows, however, that venture-backed firms experience significant and positive impacts on future growth. Thus, raising venture may overcome some of the impediments inherent in government funding relationships.

To further explore this variation, I separate and evaluate firms who receive venture before SBIR funding (ex-ante) against those who receive venture after SBIR funding (ex-post). Table 4 shows the results for logged revenue. Interestingly, firms who receive venture ex-ante experience similar impacts on future performance. However, firms who receive venture ex-post have no significant lasting adverse effect on revenue growth post-award. This directional analysis provides further support for H2. Specifically, that raising venture capital post-SBIR-award may counter-act some of the government-funding impediments. For example, venture might open new pathways for opportunity recognition, overcoming institutional impediments. However, receiving venture before award would still leave firms open to constraining institutional and structural impediments.

Table 4. Growth, Log Revenue: Diff-in-Diff

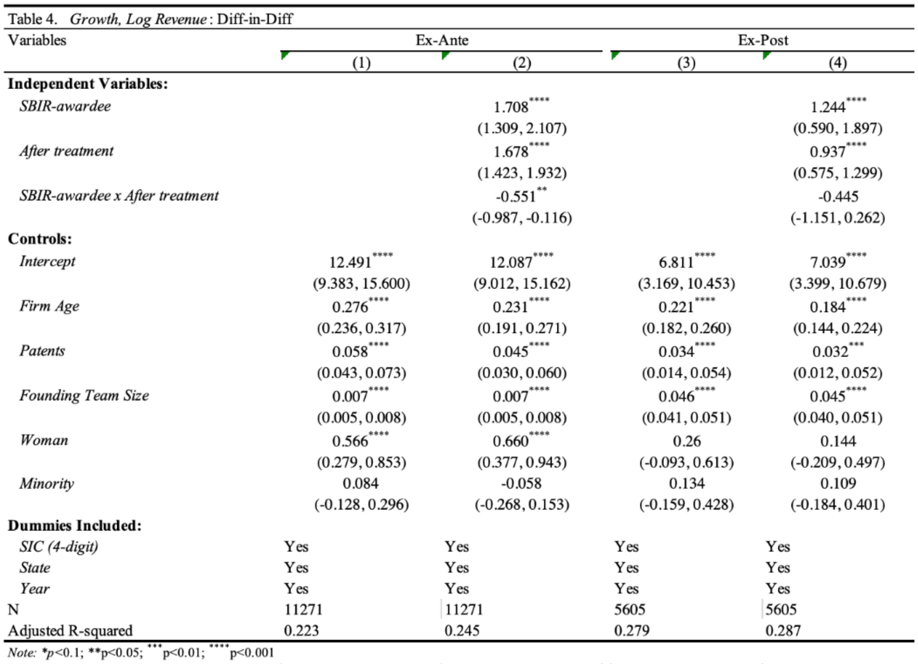


Table 4. *Growth, Log Revenue* : Diff-in-Diff

Variables	Ex-Ante		Ex-Post	
	(1)	(2)	(3)	(4)
Independent Variables:				
SBIR-awardee		1.708****		1.244****
		(1.309, 2.107)		(0.590, 1.897)
After treatment		1.678****		0.937****
		(1.423, 1.932)		(0.575, 1.299)
SBIR-awardee x After treatment		-0.551**		-0.445
		(-0.987, -0.116)		(-1.151, 0.262)
Controls:				
Intercept	12.491****	12.087****	6.811****	7.039****
	(9.383, 15.600)	(9.012, 15.162)	(3.169, 10.453)	(3.399, 10.679)
Firm Age	0.276****	0.231****	0.221****	0.184****
	(0.236, 0.317)	(0.191, 0.271)	(0.182, 0.260)	(0.144, 0.224)
Patents	0.058****	0.045****	0.034****	0.032***
	(0.043, 0.073)	(0.030, 0.060)	(0.014, 0.054)	(0.012, 0.052)
Founding Team Size	0.007****	0.007****	0.046****	0.045****
	(0.005, 0.008)	(0.005, 0.008)	(0.041, 0.051)	(0.040, 0.051)
Woman	0.566****	0.660****	0.26	0.144
	(0.279, 0.853)	(0.377, 0.943)	(-0.093, 0.613)	(-0.209, 0.497)
Minority	0.084	-0.058	0.134	0.109
	(-0.128, 0.296)	(-0.268, 0.153)	(-0.159, 0.428)	(-0.184, 0.401)
Dummies Included:				
SIC (4-digit)	Yes	Yes	Yes	Yes
State	Yes	Yes	Yes	Yes
Year	Yes	Yes	Yes	Yes
N	11271	11271	5605	5605
Adjusted R-squared	0.223	0.245	0.279	0.287

Note: *p<0.1; **p<0.05; ***p<0.01; ****p<0.001

Conclusion

In Shane’s (2000) seminal work on opportunity discovery, he suggested that there exist “wrong” opportunities for new firms. That is to say, he hypothesized that there existed an opportunity that could offer immediate support to the entrepreneurial firm, but ultimately result in unforeseen adverse consequences. Yet, since Shane, little if any work has illuminated what a “wrong” opportunity might be. For the first time, this paper illustrates one possible example, arguing that agility-constraining opportunities may provide critical resources for firm survival, but have damaging long-term consequences to firm growth.

The results of this paper illustrate a particularly exciting outcome: that while mission-oriented agency funding seems to have a constraining effect on revenue-growth, it has a positive and complementary impact on employment. Post-result interviews with entrepreneurs provided some additional context. For example, when asked, “What is the first thing you spend your SBIR funding on?” all interviewees claimed to allocate the funds towards hiring personnel. This is mostly consistent with the nature of DoD SBIR awards. By statute, all SBIR funding has to be allocated toward technically-oriented tasks. This means that SBIR funding cannot be spent on other, business growth tasks—such as sales or marketing. Given this additional information, it is easy to reconcile these differences between SBIR net revenue and net employment growth effects.

Also of interest is the impact of venture funding. The DoD instituted a SBIR “fast-track” program in 1995 to incentivize firms to pursue private capital along with SBIR funding by prioritizing the applications of firms who received third-party financing (Wessner, 2000). Reviews on the fast-track program have found that companies who receive both public and private capital experience commercialization rates five times greater than SBIR-receiving firms who do not participate in the fast-track program. This result is supported by Table 4. Therefore, while the fast-track program was initially established to keep relevant firms solvent through long contracting timelines, I argue that it has a more critical function with technology start-ups. Specifically, by incentivizing private capital, the SBIR program reduces potential institutional impediments by expanding a firm’s opportunity recognition space.

There are limitations to this research. First and foremost, although matching via strict sub-sampling provides the most accurate quasi-experimental design results, the quantitative methodology concludes only strongly-supported associations, not causal inference. Second, one should not interpret these results as being a slight towards the U.S. DoD SBIR program. There exist significant and well-supported reasons why the DoD might fund companies via agility-constraining opportunities. Although mission-oriented funding agencies support technical innovation, their application for that technology may be significantly different from commercial applications. Furthermore, military applications have a comprehensive set of rigorous safety and robustness standards that the retail market does not. Thus, although these opportunities might be constraining to entrepreneurial growth, that does not mean that they are not necessarily so.

However, important findings can be extrapolated for new policy. First, if funding agencies must employ a resource constraining opportunity, they should recognize the potentially damaging effects on technology start-ups. Instead, for those opportunities, perhaps the government should prioritize existing small business over start-up applications. Alternatively, the results indicate that if the military wishes to partner with entrepreneurial firms, it should take a less restrictive approach. Perhaps employing grants instead of contracts or allocating additional funds for firms to expand their institutional resources outside of the military market would significantly decrease negative associations between contract award and growth. Ultimately, the critical insight is that technology start-ups are different from small businesses, and should be approached as such.

References

Anton, J., & Yao, D. A. (1994). Expropriation and inventions: Appropriable rents in the absence of property rights. *American Economic Review, 84*(1), 190–209.

Archibald, R. B., & Finifter, D. H. (2003). Evaluating the NASA small business innovation research program: Preliminary evidence of a trade-off between commercialization and basic research. *Research Policy, 32*(4), 605–619.

Armanios, D. E., Eesley, C. E., Li, J., & Eisenhardt, K. M. (2017a). How entrepreneurs leverage institutional intermediaries in emerging economies to acquire public resources. *Strategic Management Journal, 38*(7), 1373–1390.

Armanios, D. E., Eesley, C. E., Li, J., & Eisenhardt, K. M. (2017b). How entrepreneurs leverage institutional intermediaries in emerging economies to acquire public resources. *Strategic Management Journal, 38*(7). https://doi.org/10.1002/smj.2575

Audretsch, D. B. (2003). Standing on the shoulders of midgets: The U.S. small business innovation research program (SBIR). *Small Business Economics, 20*(2), 129–135.

Audretsch, D. B., Link, A. N., & Scott, J. T. (2002, January). Public/private technology partnerships: Evaluating SBIR-supported research. *Research Policy, 31*, 145–158.

Audretsch, D. B., & Mahmood, T. (1995). New firm survival: New results using a hazard function. *The Review of Economics and Statistics, 77*(1), 97.

Audretsch, D. B., Weigand, J., & Weigand, C. (2002). The impact of the SBIR on creating entrepreneurial behavior. *Economic Development Quarterly, 16*(1), 32–38.

Autio, E., & Rannikko, H. (2016). Retaining winners: Can policy boost high-growth entrepreneurship? *Research Policy, 45*(1), 42–55.

Baker, T., & Nelson, R. E. (2005). Creating something from nothing: Resource construction through entrepreneurial bricolage. *Administrative Science Quarterly, 50*, 329–366.

Bakker, R. M., & Shepherd, D. A. (2017). Pull the plug or take the plunge: Multiple opportunities and the speed of venturing decisions in the australian mining industry. *Academy of Management Journal, 60*(1), 130–155.

Baron, R. A. (2007). Behavioral and cognitive factors in entrepreneurship: Entrepreneurs as the active element in new venture creation. *Strategic Entrepreneurship Journal, 1*(1), 167–182.

Baron, R. A., & Ensley, M. D. (2006). Opportunity recognition as the detection of meaningful patterns: Evidence from comparisons of novice and experienced entrepreneurs. *Management Science, 52*(9), 1331–1344.

Beckman, C. M., & Burton, M. D. (2008). Founding the future: Path dependence in the evolution of top management teams from founding to IPO. *Organization Science, 19*(1), 3–24.

Bramble, M. (2015). *Woman owned, SDVOSB, and minority owned: Are business designations necessary?*

Branscomb, L. M. (1993). National laboratories: The search for new missions and new structures. In *Empowering technology: Implementing a U.S. strategy*. Cambridge, MA: MIT Press.

Bruce, J. R., de Figueiredo, J. M., & Silverman, B. S. (2018). Public contracting for private innovation: Government capabilities, decision rights, and performance outcomes. *Strategic Management Journal, 1*(23).

Busom, I. (2000). An empirical evaluation of the effects of R&D subsidies. *Economics of Innovation and New Technology, 9*(2), 111–148.

Chatterji, A. K. (2009). Spawned with a silver spoon? Entrepreneurial performance and innovation in the medical device industry. *Strategic Management Journal, 30*, 185–206.

Congress. (1977). *Federal Grant and Cooperative Agreement Act*.

Dasgupta, P., & David, P. A. (1994). Toward a new economics of science. *Research Policy, 23*(5), 487–521.

David, P. A., & Hall, B. H. (2000). Heart of darkness: Modeling public–private funding interactions inside the R&D black box. *Research Policy, 29*(9), 1165–1183.

Doz, Y. L., & Kosonen, M. (2010). Embedding strategic agility. *Long Range Planning, 43*(2–3), 370–382.

Eberhart, R. N. (2017). Compensating conformity: Regulatory reform and legitimcy. *Academy of Management Proceedings, 2016*(1), 15425.

Eckhardt, J. T., & Shane, S. A. (2003). Opportunities and entrepreneurship. *Journal of Management, 29*(3), 333–349.

Eesley, C. (2016). Institutional barriers to growth: Entrepreneurship, human capital and institutional change. *Organization Science, 27*(5), 1290–1306.

Eesley, C. E., & Roberts, E. B. (2012). Are you experienced or are you talented? When does innate talent vs. experience explain entreprenuerial performance? *Strategic Entrepreneurship Journal, 6*(1). 207–219.

Eesley, C., Li, J. B., & Yang, D. (2016). Does institutional change in universities influence high-tech entrepreneurship? Evidence from China’s Project 985. *Organization Science, 27*(2), 446–461.

Eisenhardt, K. M. (1989). Making fast strategic decisions in high-velocity environments. *The Academy of Management Journal, 32*(3), 543–576.

Eisenhardt, K. M., & Schoonhoven, C. (1990). Organizational growth: Linking founding team, strategy, environment, and growth among U.S. semiconductor ventures, 1978–1988. *Administrative Science Quarterly, 35*(3), 504–529.

Feldman, M. P., & Kelley, M. R. (2006). The ex ante assessment of knowledge spillovers: Government R&D policy, economic incentives and private firm behavior. *Research Policy, 35*(10), 1509–1521.

Flammer, C. (2018). Competing for government procurement contracts: The role of corporate social responsibility. *Strategic Management Journal, 39*(5), 1299–1324.

Gans, J., & Stern, S. (2000). *When does funding research by smaller firms bear fruit? Evidence from the SBIR program* (NBER working paper, 7877).

Goldstein, A. P., & Narayanamurti, V. (2018). Simultaneous pursuit of discovery and invention in the US Department of Energy. *Research Policy, 47*(8), 1505–1512.

Guerzoni, M., & Raiteri, E. (2015). Demand-side vs. supply-side technology policies: Hidden treatment and new empirical evidence on the policy mix. *Research Policy, 44*(3), 726–747.

Gulati, R., & Higgins, M. C. (2003). Which ties matter when? The contingent effects of interorganizational partnerships on IPO success. *Strategic Management Journal, 24*(2), 127–144.

Guo, D., Guo, Y., & Jiang, K. (2016). Government-subsidized R&D and firm innovation:

Evidence from China. *Research Policy, 45*(6), 1129–1144.

Helfat, C. E., & Peteraf, M. A. (2015). Managerial cognitive capabilities and the microfoundations of dynamic capabilities. *Strategic Management Journal, 36*(6), 831–850.

Hellmann, T. F., & Thiele, V. (2017). Fostering entrepreneurship: Promoting founding or funding? *Ssrn*. https://doi.org/10.2139/ssrn.2908955

Hiatt, S. R., Carlos, C. W., & Sine, W. D. (2017). Manu militari: The institutional contingencies of stakeholder relationships on entrepreneurial performance. *Organization Science*.

Hillman, A. J., Zardkoohi, A., & Bierman, L. (1990). Corporate political strategies and firm performance: Indications of firm-specific benefits from personal service in the U.S. government. *Strategic Management Journal, 20*(1), 67–81.

Hitt, M. A., Ireland, R. D., Camp, S. M., & Sexton, D. L. (2001). Strategic entrepreneurship: Entrepreneurial strategies for wealth creation. *Strategic Management Journal, 22*(6–7), 479–491.

Howell, S. T. (2017). Financing innovation: Evidence from R & D grants. *American Economic Review, 107*(4), 1136–1164.

Hsu, D. H., Roberts, E. B., & Eesley, C. E. (2007). Entrepreneurs from technology-based universities: Evidence from MIT. *Research Policy, 36*, 768–788.

Ireland, R. D. (2007). Strategy vs. entrepreneuership. *Strategic Entrepreneurship Journal, 1*(1), 97–99.

Kazanjian, R. K. (1988). Relation of dominant problems to stages of growth in technology-based new ventures. *Academy of Management Journal, 31*(2), 257–279.

Klepper, S. (2002). Firm survival and the evolution of oligopoly. *RAND Journal of Economics, 33*(1), 37–61.

Knauss, D. T., Edwards, G. C., & Williams, R. (2017). *HALO report: Annual report on angel investments*.

Kropp, F., & Zolin, R. (2005). Technological entrepreneurship and small business innovation research programs. *Academy of Marketing Science Review, 2005*(6), 122–127.

Lerner, J. (1999). The government as venture capitalist: The long-run impact of the SBIR program. *The Journal of Business, 72*(3), 285–318.

Lerner, J. (2012). *The architecture of innovation*. Cambridge, MA: Harvard Business School.

Liebeskind, J. P. (1996). Technological entrepreneurship and small business innovation research programs. *Strategic Management Journal, 17*, 93–107.

Lin, H. (2016). Governance of information technology and cyber weapons. *Governance of Dual-Use Technologies: Theory and Practice*.

Link, A. N., & Scott, J. T. (2010). Government as entrepreneur: Evaluating the commercialization success of SBIR projects. *Research Policy, 39*(5), 589–601.

Mata, J., & Portual, P. (1994). Life duration of new firms author(s). *The Journal of Industrial Economics, 42*(3). 227–245.

Mowery, D. C. (2009). National security and national innovation systems. *Journal of Technology Transfer, 34*(5), 455–473.

Ott, T., Eisenhardt, K. M., & Bingham, C. B. (2017). Strategy formation in entrepreneurial settings: Past insights and future directions. *Strategic Entrepreneurship Journal, 11*, 306–325.

Pahnke, E. C., Katila, R., & Eisenhardt, K. M. (2015). Who takes you to the dance? How funding partners influence innovative activity in young firms. *Administrative Science Quarterly, 60*(4), 596–633.

Pahnke, E. C., Katila, R., & Eisenhardt, K. M. (2015). Who takes you to the dance? How partners' institutional logics influence innovation in young firms. *Administrative Science Quarterly*, 0001839215592913.

Paik, Y. (2014). Serial entrepreneurs and venture survival: Evidence from U.S. venture-capital-financed semiconductor firms. *Strategic Entrepreneurship Journal, 8*(6), 254–268.

Phillips, N., & Tracey, P. (2007). Opportunity recognition, entrepreneurial capabilities and bricolage: Connecting institutional theory and entrepreneurship in strategic organization. *Strategic Organization, 5*(3), 313–320.

Prendergast, C. (2002). The tenuous trade-off between risk and incentives. *Journal of Political Economy Journal of Political EconomyJournal of Political Economy, 110*(5), 1071–1102.

Ryu, D., Kwon, S. J., & Park, E. (2018). The influence of founders' strategic agility and dynamic capability on the opportunity pursuit process of new ventures: An exploratory case study in South Korea. *Academy of Strategic Management Journal, 17*(1), 1–17.

Sauermann, H., & Stephan, P. (2012). Conflicting logics? A multidimensional view of industrial and academic science. *Organization Science, 24*(3), 889–909.

SBA. (2014). *The SBIR and STTR Program Interagency Policy Committee Report to Congress*.

Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). *Experimental and quasi-experimental designs for generalized causal inference*. Boston, MA: Wadsworth Cengage Learning.

Shane, S., & Venkataraman, S. (2000). The promise of entrepreneurship as a field of research University of Maryland. *Academy of Management Review, 25*(1), 217–226.

Short, J. L., & Toffel, M. W. (2010). More than merely symbolic: The critical environment. *Administrative Science Quarterly, 55*, 361–396.

Söderblom, A., Samuelsson, M., Wiklund, J., & Sandberg, R. (2015). Inside the black box of outcome additionality: Effects of early-stage government subsidies on resource accumulation and new venture performance. *Research Policy, 44*(8), 1501–1512.

Stern, S., Porter, M., & Furman, J. (2000). *The determinants of national innovation capacity*, 3, 56.

Stuart, E. A. (2010). Matching methods for causal inference: A review and look forward. *Statistical Science, 25*(1), 1–21.

Suarez, F. F., & Ulterback, J. M. (1995). Dominant designs and the survival of firms. *Strategic Management Journal, 16*(6), 415–430.

Thornton, P. H., Ocasio, W., & Lounsbury, M. (2012). *The institutional logics perspective: A* *new approach to culture, structure, and process*. Oxford University Press on Demand.

Wallsten, S. J. (2000, Spring). The effects of government–industry R & D programs on private R&D: The case of the small business innovation. *RAND Journal of Economics, 31*(1), 82–100.

Wang, H., & Qian, C. (2011). Corporate philantrhopy and corporate finacial performance: The roles of stakeholder response and political acess. *Academy of Management Journal, 54*(6), 1159–1181.

Wang, Y., Li, J., & Furman, J. L. (2017). Firm performance and state innovation funding: Evidence from China’s Innofund program. *Research Policy, 46*(6), 1142–1161.

Wessner, C. W. (2000). The small business innovation research program: An assessment of the Department of Defense fast track initiative. *National Academy Press*. https://doi.org/10.17226/9985

Zajac, E. J. (1988). Interlocking directorates as an interorganizational strategy: A test of critical assumptions. *Academy of Management Journal, 31*(2), 428–438.

An Analytic Model of Success for Information Technology Decision Making

T. M. Clemons, III—George Mason University, Department of Systems Engineering and Operations Research [tclemons@gmu.edu]

KC Chang—George Mason University, Department of Systems Engineering and Operations Research [kchang@gmu.edu]

Sean Tzeng—George Mason University, Department of Systems Engineering and Operations Research [sean.tzeng@outlook.com]

Abstract

Developing an information technology (IT) system to meet organizational needs is complicated, is often very extensive, takes a long time to realize, and is almost always costlier and more difficult than originally planned. To help with this complexity, many businesses use the Information Technology Infrastructure Library (ITIL)® to guide the design, procurement, and operation of their IT systems. The ITIL is intended to optimally synchronize IT departments to function in accordance with the needs of the business. To further assist managers in monitoring the progress of their IT programs we developed a Bayesian Network stochastic model, the IT Decision Management System (ITDMS), to simulate the program's evidence observations, complex interrelationships, and the dynamic/temporal relationships. Based on the Defense Business Systems Acquisition Probability of Success (DAPS) Model, a technical framework developed at George Mason University, the model aligns the sub-process of each ITIL phase in a Bayesian structure that allows a decision maker to assess program performance in specific subject matter knowledge areas and the overall likelihood of program success by considering both data and temporal uncertainty. The key difference between DAPS and ITDMS is the explicit incorporation of the utility and decision factors in the Bayesian influence diagram model.

Introduction

Information technology system development and management came to the forefront of the U.S. federal government in 1996 when the Clinger-Cohen Act was signed into federal law, mandating oversight and management of Information Technology. The issues were that many of the Enterprise Resource Planning (ERP) Defense Business System (DBS) acquisition programs were too big, too complex, and too time-consuming (GAO, 2012). It is clear that developing an information technology (IT) system to meet organizational needs is not a simple task. It is often very extensive, takes a long time to realize, and is almost always costlier and more difficult than originally imagined. This is especially true for large IT projects. It was reported that on average (based on 5,400 IT projects), large IT projects run 45% over budget, 7% over time, and are delivered with 56% less value (Bloch, Blumberg, & Laartz, 2012). A Government Accountability Office (GAO) report also indicates that of 10 Enterprise Resource Planning (ERP) programs the Department of Defense (DoD) identified as critical to business operations transformation, nine programs were experiencing schedule delays up to six years, and seven programs were facing estimated cost increases over $2 billion (GAO, 2012). This occurred even though there were strict acquisition laws, regulations, policies, guidance, independent assessments, as well as technical reviews and milestone reviews to guide DBS acquisitions. A significant amount of data and large numbers of artifacts such as Program Schedule, Earned Value Management System (EVMS) Metrics, Business Case, and Systems Engineering Plan are generated during execution of DBS programs. These data/artifacts are commonly used by decision makers at technical reviews and milestone reviews as evidence of program progress to support their acquisition decisions. However, the evidence by itself is, by nature, incomplete, ambiguous, unreliable, and often conflicting (Schum, 2001; Laskey, 2012), making integration of the evidence to finalize decisions a challenging endeavor.

The most challenging issue is that there is often an abundance of data and evidence, but limited analytical tools to figure out what all the evidence means collectively, and how they support the hypothesis being sought. Good decision-making requires not only information and evidence, but also the inference and representation of the evidence to support the decision. There are currently limited means to aid DBS acquisition decision makers holistically and logically process all the available evidence efficiently and limited means to assimilate all evidence to identify program critical areas and the likelihood of achieving program success. This problem is not different from what other disciplines experience in a wide range of enterprises and in private sectors such as social services, transportation, and health care systems.

To assist in managing this problem, a Probability of Program Success (PoPS) model developed in 2005 with a goal of identifying a program’s health using a scoring system (Department of Navy, 2012). While the PoPS model provides a logical framework to assess an acquisition program, the system aggregates the scores in a hierarchical manner and does not have a mechanism to model uncertainty or the complex interrelationships between key driving factors. In addition, PoPS is designed to represent a snapshot of the current status of the program; it does not factor in the past scores or how the current scores might affect the future scores. In other words, there is no built-in dynamic model in PoPS to predict the probability of failure at a later stage of the program.

To address these issues, a Defense Business System Acquisition Probability of Success (DAPS) was developed (Tzeng, 2015; Tzeng & Cheng, 2015) to enhance the qualitative framework of PoPS with a sophisticated quantitative reasoning approach. DAPS is an expert-based model constructed using probabilistic graphical models (i.e., Bayesian Networks; Steven 2014; Khodakarami; 2009) to help decision makers collectively process the available evidence produced during DBS acquisition. Based on observations and inferences of evidence, the DAPS model can assess project performance in specific subject matter knowledge areas (KAs) and assess the overall likelihood for program success.

DAPS was specifically designed for Defense Business System (DBS) acquisition applications to assess program success with no explicit linkage to decision makers’ subjective utility or recommended actions/decisions. This research aims to provide IT business managers a decision support tool by augmenting the DAPS with the popular Information Technology Infrastructure Library (ITIL) model. The key difference between the resulting Information Technology Decision Management System (ITDMS) and DAPS is the explicit incorporation of the utility and decision factors in the Bayesian influence diagram model as well as the incorporation of the ITIL process. It allows a decision maker to assess program performance at important checkpoints with recommended actions and the resulting likelihood of program success by considering both evidence and temporal uncertainty.

Background Research

Motivations and Background

Large business acquisition programs experience a great deal of complexities, difficulties, and inefficiencies. Acquisition professionals, including systems engineers and project/program managers, constantly have to manage the scope, cost, schedule, and system quality of a project while trying to meet statutory and regulatory acquisition requirements. However, many of the system’s life cycle risks are currently assessed subjectively by imprecise qualitative methodologies and subsequently suffer from unforeseen failures as well as cost and schedule overruns. This is particularly the case for DBS and large IT systems where many programs critical to business operation transformation experience major schedule delays and/or significant cost increases (Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics [OUSD(AT&L)], 2006).

To improve acquisition program performance, the GAO recommends a knowledge-based acquisition framework for DBS (GAO, 2015). The GAO report states,

> A knowledge-based approach to product development efforts enables developers to be reasonably certain, at critical junctures or ‘knowledge points’ in the acquisition life cycle, that their products are more likely to meet established cost, schedule, and performance baselines and, therefore provides them with information needed to make sound investment decisions. (GAO, 2015)

In short, sufficient knowledge reduces the risk associated with the acquisition program and provides decision makers and program manager higher degrees of certainty to make better decisions.

The concept of the knowledge-based acquisition is fully adapted in this research and built into the ITDMS model. With the perspective of a program manager, the goal of the research is to develop a probabilistic reasoning quantitative system using a graphical model (Bayesian Networks) to facilitate evidence-based decision making for an IT acquisition process (Steven, 2014; Khodakarami, 2009). The previously developed DAPS model is extended by expanding the body of domain knowledge and adapted to IT and engineered system programs in general. In particular, to align information technology services with the needs of business, the ITIL model is incorporated into the overall system.

The resulting ITDMS model could model processes, procedures, knowledge areas, and performance checklists as described by ITIL process that are not organization-specific but can be applied by any organization to ensure delivering value and maintaining competency. It could help systems engineers, program managers, and decision makers better analyzing the available data/evidence in relation to project success and thus make better decisions. ITDMS can be applied to support the difficult acquisition decisions to continue projects that will be successful and discontinue projects which will not, subsequently, maximize return on investment in large scale IT acquisition process.

Bayesian Network and Knowledge Representation

Bayesian Network (BN) is a formal language for representing knowledge about uncertain quantities. It is based on the Bayesian approach of probability and statistics, which considers prior belief and uses probability inference to update belief based on observed evidence. Bayesian Networks are direct acyclic graphs that contain nodes representing hypotheses, arcs representing direct dependency relationships among hypotheses, and conditional probabilities that encode the inferential force of the dependency relationship (Neapolitan, 2004).

A BN is a natural representation of causal-influence relationships (CIRs), the type of direct dependency relationships built in the DBS DAPS model where CIRs are relationships between an event (the cause) and a second event (the effect). BN was used to construct the DAPS model, assessing the observable evidence and make inference on the probability to meet the cost, schedule, performance quality, and scope goals. The evidence within the framework of an acquisition program includes the artifacts, technical plans, facts, data, and expert assessments that will tend to support or refute the hypothesis of program success. Evidential reasoning utilizes inference networks to build an argument of the observable evidence items to the hypothesis being sought (Liu, Yang, & Sii, 2002). For the case of DBS acquisition, the DAPS model argues for the hypothesis of program success or the alternative hypothesis of program failure based on the observations of evidence.

DAPS Bayesian Network Model

DAPS was developed with a BN model using the Netica software tool (Netica, 2015). By using BN, DAPS was able to construct a complex inference network to measure the uncertainties in subject matter knowledge areas, assess the level of success achieved at knowledge checkpoints, and predict the likelihood for future program success or failure.

The DAPS BN model contains a three-level structure, representing the three types of nodes/variables in the model. There are also three types of static arcs representing the interrelationships among the variables at a point in time, and one type of dynamic arc representing the temporal relationships from one point in time to another. For example, Figure 1 shows the DAPS model at the first knowledge checkpoint, Material Development Decision (MDD).

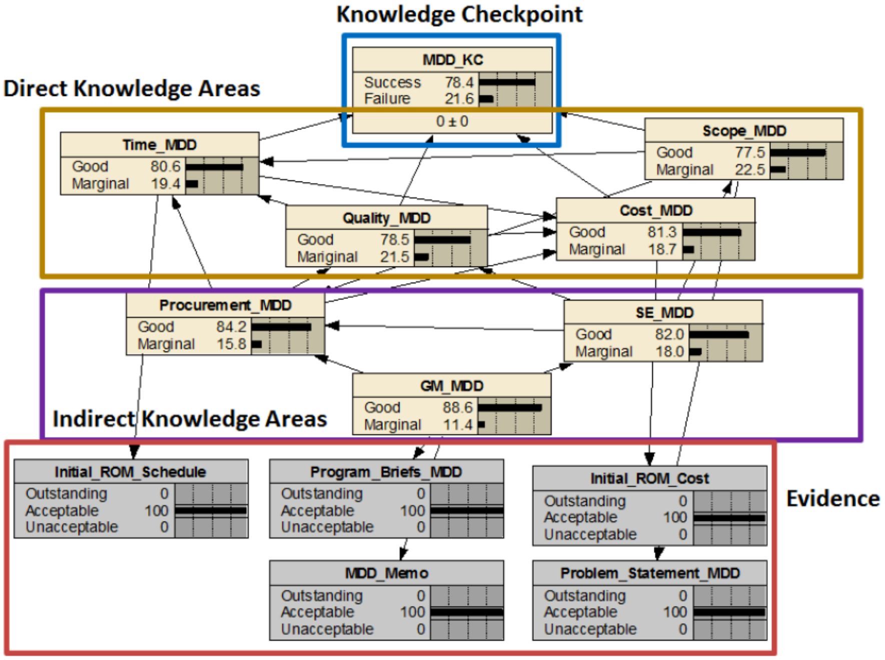


Figure 1. **DAPS Knowledge Inference Structure**
(Tzeng & Chang, 2015)

The knowledge checkpoint is the top-level node which cumulates all information about the DBS acquisition program at that decision point, assessing the likelihood of program success. It provides a cumulative measurement of success achieved by the program up to the current knowledge checkpoint and is the metric that decision makers can use to help decide whether the program has demonstrated enough certainty and maturity to move on to the next phase of the acquisition program. Knowledge checkpoints contain four knowledge area nodes as parent nodes: time, quality, cost, and scope knowledge areas. They represent the four direct measures of success which is defined in DAPS as meeting program time, cost, and quality goals within the program scope. There are 15 technical reviews and milestone reviews that align with the DBS acquisition process modeled in DAPS as knowledge checkpoints (Defense Acquisition University, 2003; Project Management Institute, Inc., 2008). Each knowledge checkpoint nodes contain two states describing the state of the program: “success” and “failure.” The probability of these states reflects the assessment of the program performance at the knowledge checkpoint.

Knowledge areas are the second-level node that measures the certainty and maturity attained for that particular subject matter area of DBS acquisition at the knowledge checkpoint. Knowledge areas in DAPS are derived from the nine Project Management Body of Knowledge (PMBOK) knowledge areas (Defense Acquisition University, 2003; Project Management Institute, Inc., 2008), integrated with the systems engineering elements of defense acquisition. It is further divided into the measurable (direct) and enabling (indirect) knowledge areas. Measurable knowledge areas include scope, cost, time, and quality subject matter areas which directly affect the measures of program success in DAPS. Enabling knowledge areas include general management, systems engineering, and procurement subject areas that do not directly affect the measure of program success, but however are important enabling factors that drive success.

The dynamic arcs, starting from the knowledge area node at the prior knowledge checkpoint to the same knowledge area node at the posterior knowledge checkpoint, model the relationships of DBS acquisition through time. It represents the knowledge in a knowledge area at the prior checkpoint influencing the knowledge of the same knowledge area at the next checkpoint. DAPS uses knowledge area nodes to model the dynamic effects in the progression of knowledge during an acquisition project. Thus, each knowledge area node gains information from the observations at the current knowledge checkpoint, as well as the information cumulated from prior knowledge checkpoints. Figure 2 provides an example graph of the dynamic arcs in green arrows from the Material Development Decision knowledge checkpoint to the next Initial Technical Review knowledge checkpoint.

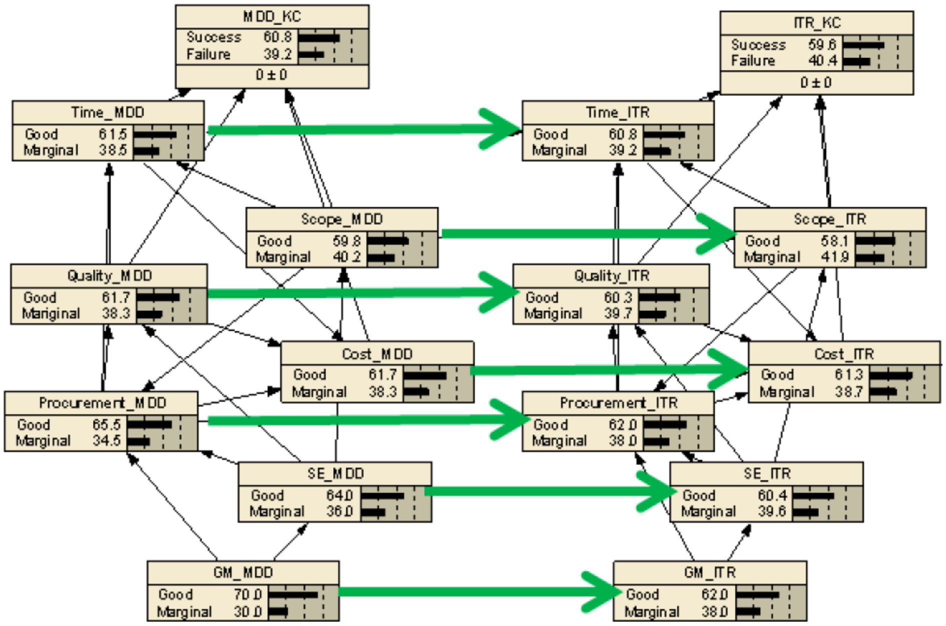


Figure 2. **Knowledge Area to Knowledge Area Dynamic Arcs Example (Tzeng & Chang, 2015)**

The third and bottom-level nodes are the evidence nodes in the DAPS model. Observations of evidence are entered here at this level to drive inference for assessing a program’s probability of success. The only CIRs for this level are the arcs from knowledge area nodes to evidence nodes. Evidence nodes contain three states describing the state of the evidence: “outstanding,” “acceptable,” or “unacceptable.” These states reflect the risk assessment of the program in the specific knowledge area. Since these are the observation nodes, one of the states is chosen to describe the real-world observation of the evidence. This provides information to update the belief in the parent knowledge area.

The knowledge area nodes then propagate the information to combine the belief based on the evidence observed under the knowledge area, as well as the belief in other knowledge areas where there is a CIR relationship. Finally, the direct knowledge areas provide information to the knowledge checkpoint node to assess the belief in the knowledge checkpoint node states (success, failure), which completed the information flow within a static knowledge checkpoint. The information at the knowledge checkpoint is then passed on to the next knowledge checkpoint utilizing the seven knowledge area nodes through the dynamic arcs, where evidence node assessment observations will again be made. The information flow process is then repeated multiple times until the last knowledge checkpoint, Full Operating Capability (FOC), is reached.

Decision Theoretic Approach With Bayesian Decision Networks

To incorporate utility and decision factors into the DAPS model, we adopt an Influence Diagram (ID) (also called Bayesian Decision Network [BDN]) to enhance the DAPS model (Yoo, 2007). A BDN is a directed acyclic graph consisting of three types of nodes: decision, state, and value nodes. Decision nodes represent the decisions to be made and their set of possible alternatives. State nodes represent uncertain variables or hypotheses relevant to the decision problem. Value nodes are associated with decision and state nodes to characterize their benefits and costs. Arcs between two nodes represent their probabilistic causal influence or deterministic relationship. Figure 3 shows a simple BDN to represent various components related to R&D investment decision-making where the utility/value node representing benefits (market value) of the actions.

Within BDN, the uncertainties and dependences among the state and decision variables are systematically captured by its explicit graphical representation, making it ideal for modeling decision problems such as the one in ITDMS. A BDN is able to update (assess or predict) the probabilities of the states of a variable given observation (evidence) from other related nodes. To facilitate efficient probabilistic inference for optimal decision, a decision-theoretic framework is adopted to evaluate and compare the expected utility of each decision (Zhang & Ji, 2006). The framework provides solid theoretical foundations and has the capabilities of integrating evidence and knowledge in a principled manner. In the framework, an optimal decision is the one that maximizes the overall expected utility.

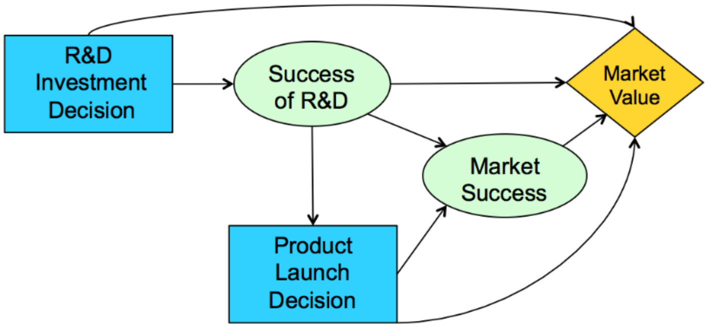


Figure 3. **A BDN for Modeling Product Investment Decision Making Under Uncertainty**

Modeling and Analysis

ITIL Model Description

The Information Technology Infrastructure Library (ITIL) is a well-known industry-standard for IT and cloud services (Gray, 2006). The ITIL functions as a guide to system lifecycle management of IT systems, including acquisition and operations. ITIL helps organizations across industries offer their services in a quality-driven and economical way. The ITIL standard is a set of five volumes of guidelines that largely leave the implementation of the process up to the organization (Clydebank Technology, 2017; Agutter, 2012). As shown in Figure 4, the five main components of the ITIL service lifecycle cover various other sub-categories, including demand management, capacity management, release management, incident management, event management, etc. They are meant to cover all areas of IT service management.

A core component of the ITIL model is the service strategy design, transition, and operation (Taylor, 2011). The goal is to provide a strategy for the service lifecycle in sync with the customer's business objectives as well as to manage services within its scope. The strategies are designed to ensure that the service is fit for purpose and fit for use in order to add value to the customers. There are many benefits of using ITIL, such as lower operating costs, increased awareness of IT infrastructure status, higher customer satisfaction, and better help/service desk response. Furthermore, the non-proprietary and heterogeneous nature of ITIL enables it to be applied in almost any organization (Gray, 2006). Because of these benefits, ITIL has become a standard in IT service management and is experiencing significant growth and awareness worldwide.

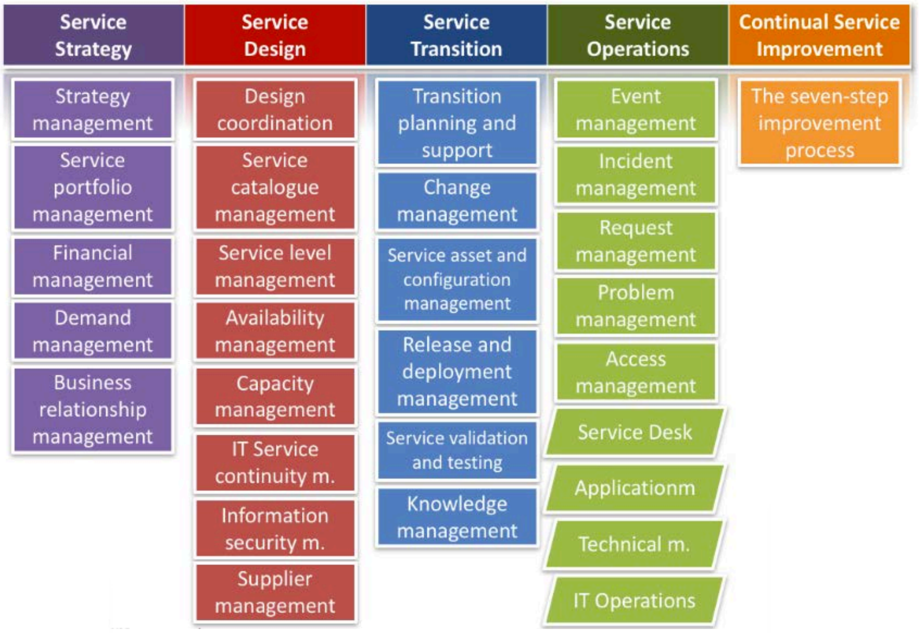


Figure 4. **ITIL Components for Service Management**
(Taylor, 2011)

ITDMS Model Specifications

The ITIL library (Clydebank Technology, 2017; Agutter, 2012) provides a set of detailed practices for IT service management. In the ITIL system, the broad lifecycle phases serve a similar function as the review phases in the defense acquisition process Defense Acquisition University, 2013; DoD, 2013). It was pointed out specifically that success or failure of ITIL implementations is hard to define and that strong project management is a key to implementation (Gray, 2006). Lengthy implementation, high risk, and the need for senior leader involvement can be surmounted through a formal approach to tracking and evaluation of progress. This problem directly involves the Systems Engineering disciplines of Project Assessment and Control, Decision Management and Risk Management. To help overcome these difficulties, we integrate the ITIL library with the DAPS model to develop ITDMS.

As in DAPS, in ITDMS the knowledge checkpoints are the project success indicators at certain stages of the acquisition process. However, unlike the 15 stages used in DAPS, in ITDMS, four of the five ITIL processes make up the knowledge checkpoints (KCs) from the DAPS model. Specifically, the four checkpoints are as follows:

- Service Strategy (SVC_STRAT_KC)
- Service Design (SVC_DSGN_KC)
- Service Transition (SVC_XSN_KC)
- Service Operation (SVC_OPS_KC)

These four ITIL lifecycle phases roughly correlate to the Initial Technical Review (ITR), Preliminary Design Review (PDR), Initial Operational Capability (IOC), and System Final Review (SFR) of the defense acquisition process in DAPS. The fifth process, Continual Service Improvement, does not fit into the construct of a checkpoint in that the process is ongoing and cyclical, representing an already fielded system and not a new development/deployment. This process might be addressed through a series of ongoing cyclical knowledge checkpoints, however, that option is not addressed herein, but could form an area of future work. As an aside, one might notice how the above processes closely align with the Systems Engineering phases of Concept Development, Production, and Utilization and Support.

Although the ITIL processes are meant to cover a particular phase of IT service management, and the reviews mentioned above are approval points, the activities and measurements conducted during each of the individual ITIL processes correlate with the activities one would perform prior to the decision to move to the next phase of an acquisition cycle. As shown in Figure 4, each of the ITIL phases have a number of formal processes, sub-processes, procedures, tasks, and checklists that are applied by an organization to successfully integrate new or updated IT functions (Gray, 2006; Clydebank Technology, 2017; Agutter, 2012; Taylor, 2011).

In the ITDMS we use these process outputs as evidence supporting the knowledge areas that inform the knowledge checkpoint. As with the DAPS model, the knowledge areas in ITDMS represent the complex interrelationships of a successful program and organize the evidence of sub-processes, as well as provide input to the knowledge checkpoint. The seven knowledge areas are further defined into measurable (direct) knowledge areas, which can be considered direct and qualitative measures of success, and enabling (indirect) knowledge areas, which although qualitatively measurable, are considered as an enabling factor to success (Tzeng, 2015). Seventeen procurement subject matter experts were interviewed to collect the necessary data for network structure and probability specification for the model (Tzeng & Cheng, 2015). The subject matter experts (SME) opinions were converted into the conditional probability tables associated with the knowledge areas.

The measurable (direct) knowledge areas to knowledge checkpoint are as follows:

- Time Management—schedule plan, schedule progress, schedule performance, earned value schedule metrics

- Cost Management—cost estimate, cost expenditure, cost performance, earned value cost metrics
- Scope Management–Scope of project—objectives, goals, requirements and specifications, work performance requirements
- Quality Management—product performance, defects, product verification, validation, acceptance, product supportability, data deliverable

Direct knowledge areas are considered directly measurable, where the effects of the knowledge area can be directly quantified and are considered an indicative measure of final project success outcome. Indirect knowledge areas are not considered directly measurable to project success, where the effects of the knowledge area are not easily quantifiable and are not commonly used as a measure of final project success outcome.

The enabling (indirect) knowledge areas to knowledge checkpoints are as follows:

- Procurement Management—planning and execution, contract solicitation, contract terms, software licensing agreements
- Systems Engineering Management—project integration, project risk
- General Management—staffing and human resources management, communication, environmental management, budgeting and funding, project management plan, program charter

ITDMS Model Development

In ITDMS the evidence nodes of the DAPS model are replaced by the process and sub-processes associated with each of the ITIL services. The linkages to the knowledge areas were determined by a review of the sub-processes and metrics associate with the respective ITIL process. For instance, the financial planning sub-process for service strategy knowledge checkpoint provides evidence of the cost knowledge area.

The ITDMS is enhanced by adding two decision nodes and the associated value/utility nodes to each knowledge checkpoint. The first decision is whether to conduct a separate review of the program in addition to the evidence used to determine the probability of a success or failure of the program. If it looks like the program is going to be successful from the evidence, the model does not recommend a review. However, if the program evidence indicates that there is a possibility of failure, the program manager may decide to conduct an independent review. There are three types of reports that may come out of the review; a positive report, a negative report, or no report, where the no report is included for completeness. The cost and time knowledge areas provide the evidence of the type of report given. Since a review costs money and time, there is a value associated with the review and the value node “Conduct_Review_Value” accounts for this value in the model.

The next decision required of the program manager, based on the knowledge checkpoint success/failure rating and the review recommendation, is whether to continue with the project. In this case, there are three choices: continue the project as it is, continue the project with modifications to the schedule or budget, or do not continue the project. The decision to continue the project also has a value and the “Continue_Project_Value” node of the mode accounts for this value. The project probability of success, the review recommendation, and a decision to continue the project determine the value of the recommendation. For example, the value table reflects this with a high value given for a project that has a high success rate, receives a positive review report, and is chosen to continue. Figure 5 shows the ITDMS at the Service Strategy knowledge check point with the conduct review and continue project decision nodes. The complete DBN model is shown in Figure 6 where the interconnections between the phases can be seen explicitly.

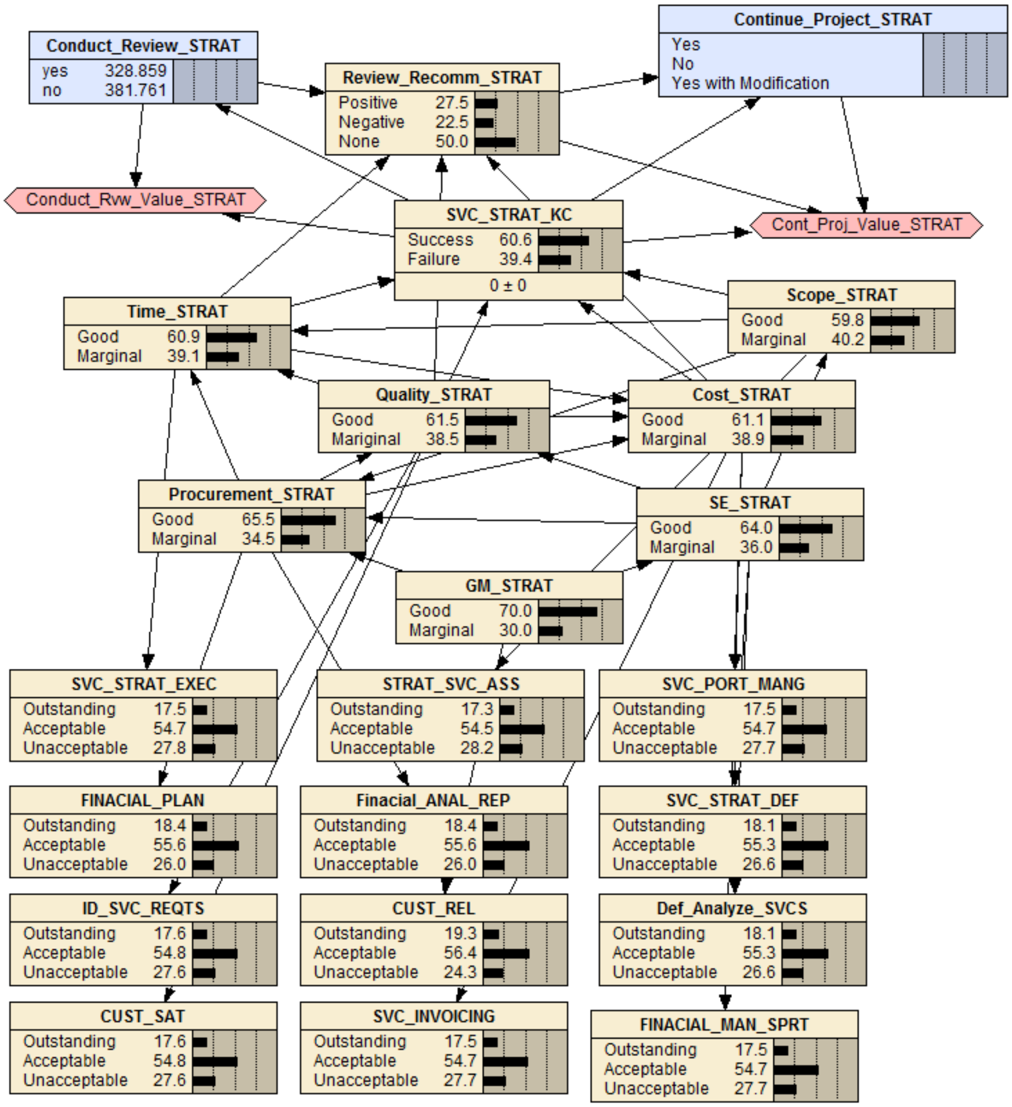


Figure 5. **ITDMS Model at the Service Strategy Knowledge Checkpoint**

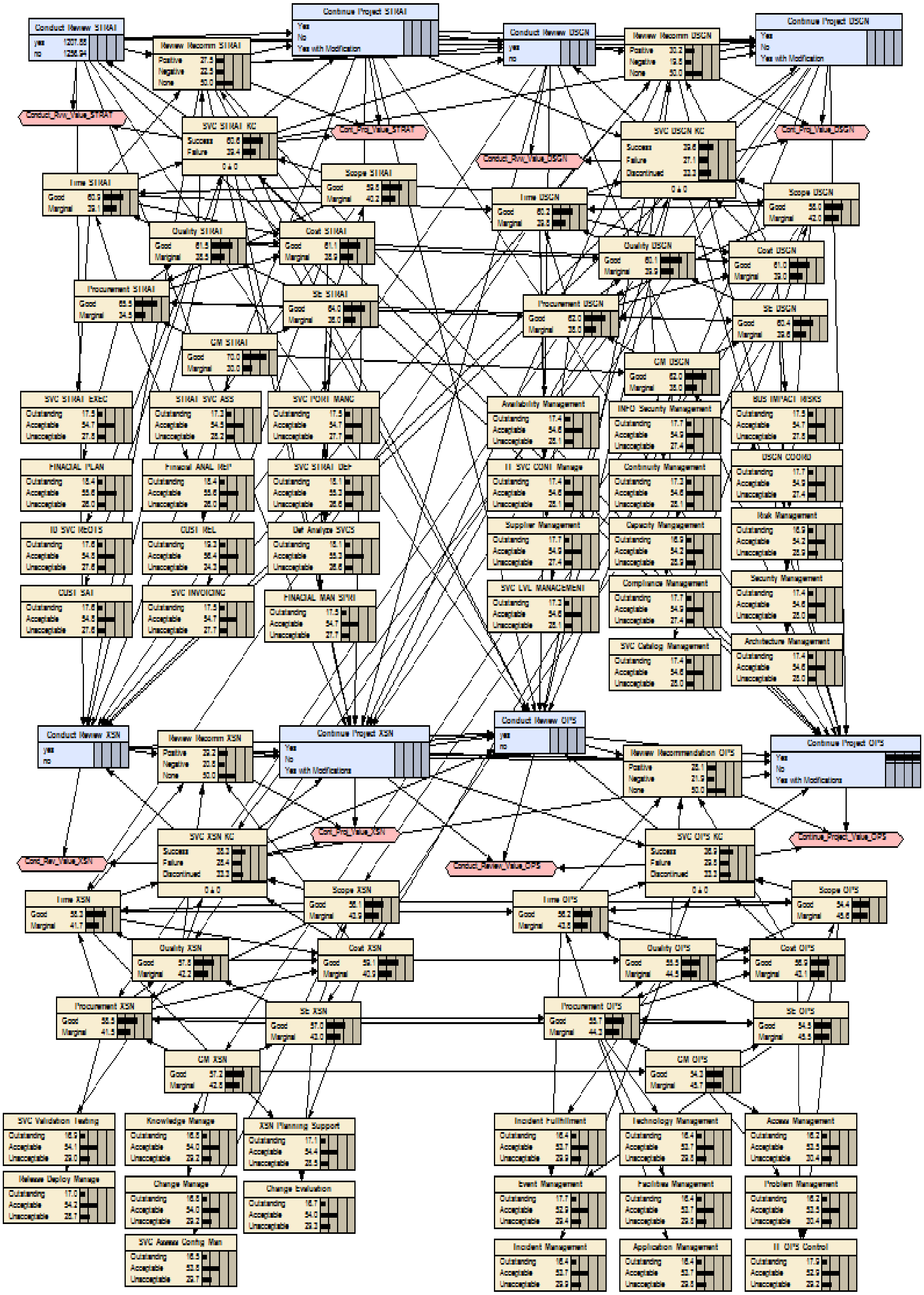
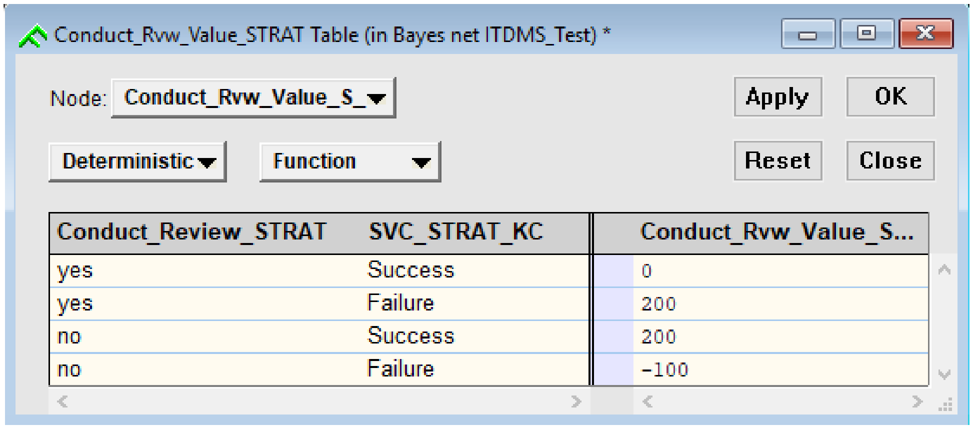


Figure 6. **The Complete ITDMS Model**

Scenarios and Case Study

We developed several scenarios to demonstrate the functionality of the ITDMS model. For example, in a scenario where a company has chosen to significantly upgrade their existing IT systems and will use ITIL as a guiding principle. Although the company can choose which sup-processes they want to use, for completeness in demonstration we will assume that the company will use all sub-processes associated with each ITIL phase. In setting up the BN for their acquisition project, the leadership of the company has assigned subjective utility values for their decision nodes. For example, Figure 7 shows the values assigned for the decision of whether to conduct an additional review of the program in the Service Strategy phase. Due to the time and cost associated with a review, there is a positive value assigned to a successful program not requiring a review. Likewise, a review is most important when a program that is in threat of failure, so the managers also assigned a high value for a conducting a review of a failing program. Conversely, a negative value is assigned to the case where a review would not be conducted for a failing program. Finally, conducting a review of a successful program will not necessarily be good or bad, so a neutral value (0) is assigned to that choice.

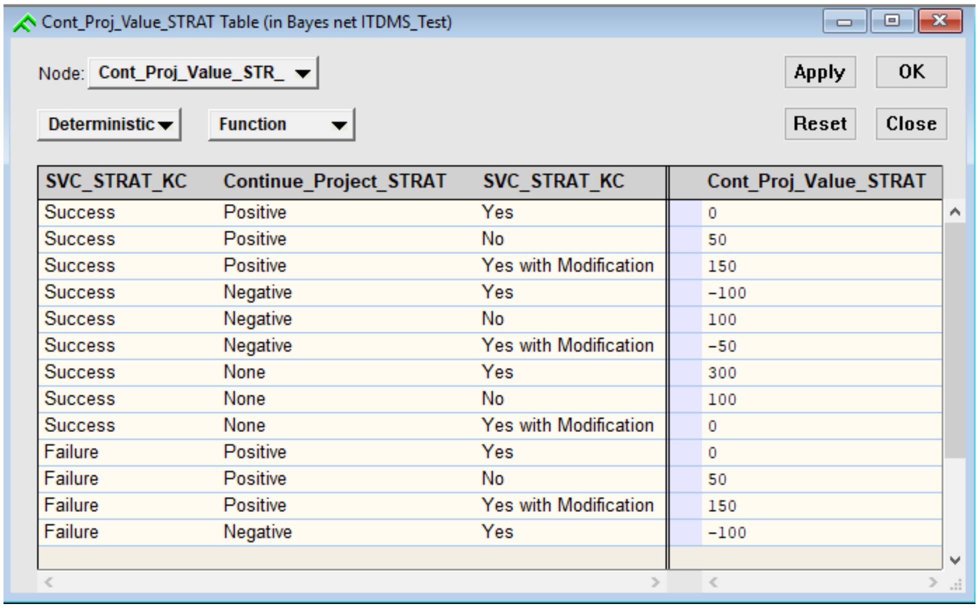
Similar reasoning is followed for the decision whether to continue with the program given the probability of program success and the results of a review if one were conducted. Because there are two inputs to this decision (knowledge checkpoint and review results) the set of values is much more complex. In summary, most value is associated with continuing a successful project and terminating a program in trouble. Relatively high value is assigned to continuing a program with some modifications, such as extra resources or timeline changes if a positive review is received on a failing program. An example of the assigned values is shown in Figure 8.


Conduct_Rvw_Value_STRAT Table (in Bayes net ITDMS_Test) *
Node: Conduct_Rvw_Value_S_
Apply
OK
Deterministic
Function
Reset
Close

Conduct_Review_STRAT	SVC_STRAT_KC	Conduct_Rvw_Value_S...
yes	Success	0
yes	Failure	200
no	Success	200
no	Failure	-100

Figure 7. **Values Assigned to Decision Value Node for Program Review**

Let's suppose that after completing some initial work developing their Service Strategy, the program manager conducts a review of progress to date. In our scenario the program has a mixture of two outstanding, seven acceptable, and three unacceptable sub-processes. Since a majority of the sub-processes are satisfactory or better, all the knowledge areas show a high probability of "Good" progress and the model predicts the program has a 70% probability of success (see Figure 9). Due to this high chance of a successful program, the model places a higher value (1,351 vs. 1,221) on not conducting a program review. Let's say that the decision maker follows the model's advice and decides not to conduct a further review and that option is chosen in the model. The result is that the model then places a higher value on continuing the project (Yes: ~1,200; No: ~900; Yes, with modification: ~1,100; see Figure 10). It should be noted that there is no reason that the program status be accessed only once during the phase. The program manager can use this assessment periodically or as situations warrant throughout the program.



Cont_Proj_Value_STRAT Table (in Bayes net ITDMS_Test)
Node: Cont_Proj_Value_STR_
Apply
OK
Deterministic
Function
Reset
Close

SVC_STRAT_KC	Continue_Project_STRAT	SVC_STRAT_KC	Cont_Proj_Value_STRAT
Success	Positive	Yes	0
Success	Positive	No	50
Success	Positive	Yes with Modification	150
Success	Negative	Yes	-100
Success	Negative	No	100
Success	Negative	Yes with Modification	-50
Success	None	Yes	300
Success	None	No	100
Success	None	Yes with Modification	0
Failure	Positive	Yes	0
Failure	Positive	No	50
Failure	Positive	Yes with Modification	150
Failure	Negative	Yes	-100

Figure 8. **Values Assigned to Continuing Project Value Node**

With the assumption that the decision maker has chosen to continue the project and we have proceeded to the Service Design Phase. A few months into this phase, the project manager again calls for another program assessment. However, here we find that things in our scenario are not going as well. Let's say here that the program has taken a turn for the worse and now several sub-processes in the Service Design Phase have unacceptable ratings (2 outstanding, 8 acceptable, 4 unacceptable) as shown in Figure 11. Many of the knowledge areas are now "Marginal" and this has pushed the probability of program success down to 43%. The model now places more value in conducting an in-depth review (~750 vs. ~650 in favor of review). If the program manager follows this recommendation and chooses to conduct the review, we find that there is a 66% probability the review will be negative.

Finally, let's assume the review is conducted, but shows that, with some changes to the program funding, it will be successful. We'll consider this a positive review recommendation and the model recommends continuing the project with modifications. The decision maker chooses to provide additional funding to the project and thus continue the project with modifications (see Figure 12). These modifications could include schedule changes, budget adjustments, or personnel changes as the program manager and decision makers see fit. On the contrary, if the review did come back negative, the Continue Project decision node would reflect more value to ending the program. Again, the program manager can opt to proceed to the next phase, Program Transition, or remain in the Design Phase and conduct another program assessment after changes are made.

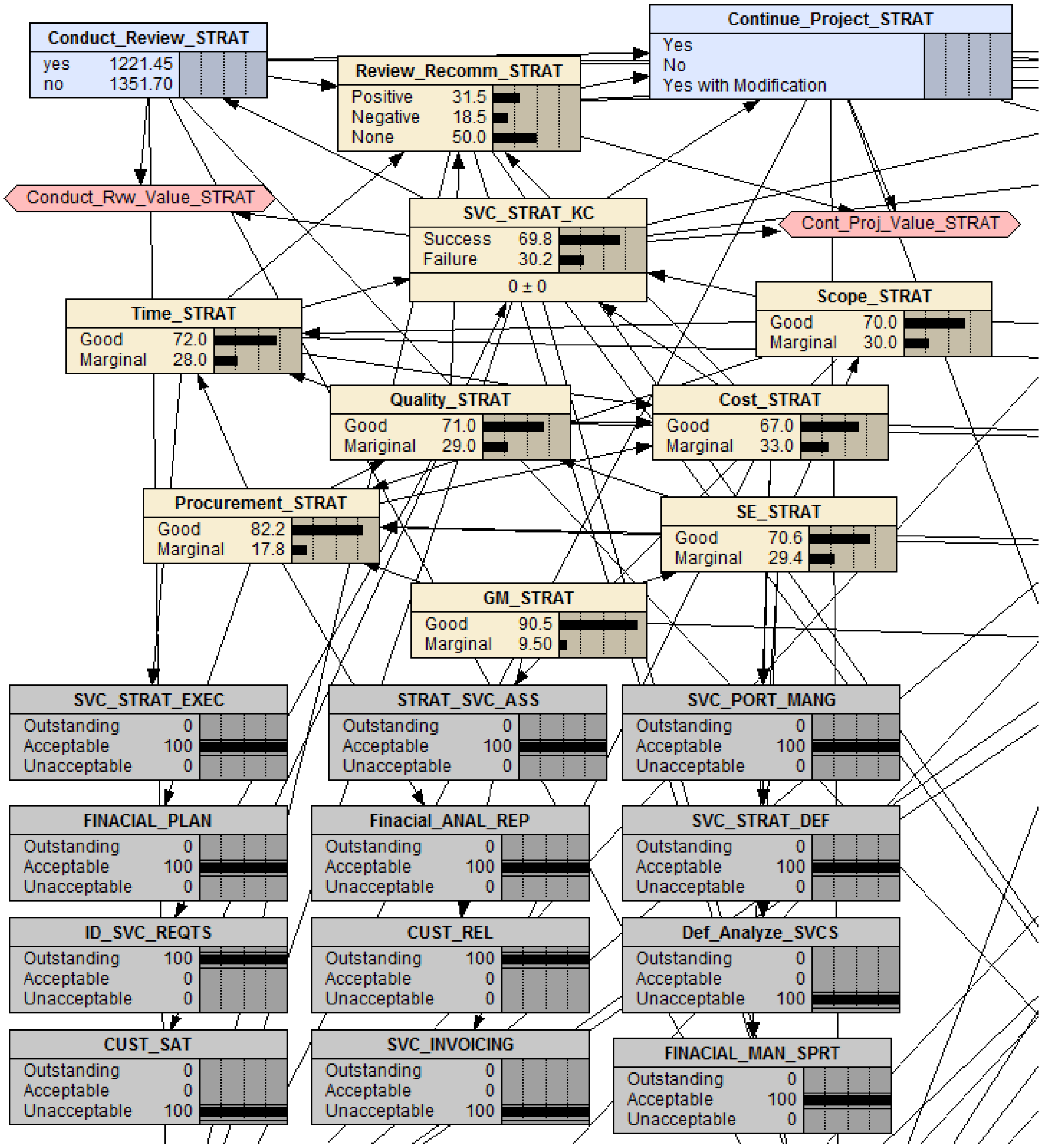


Figure 9. **Service Strategy Scenario**

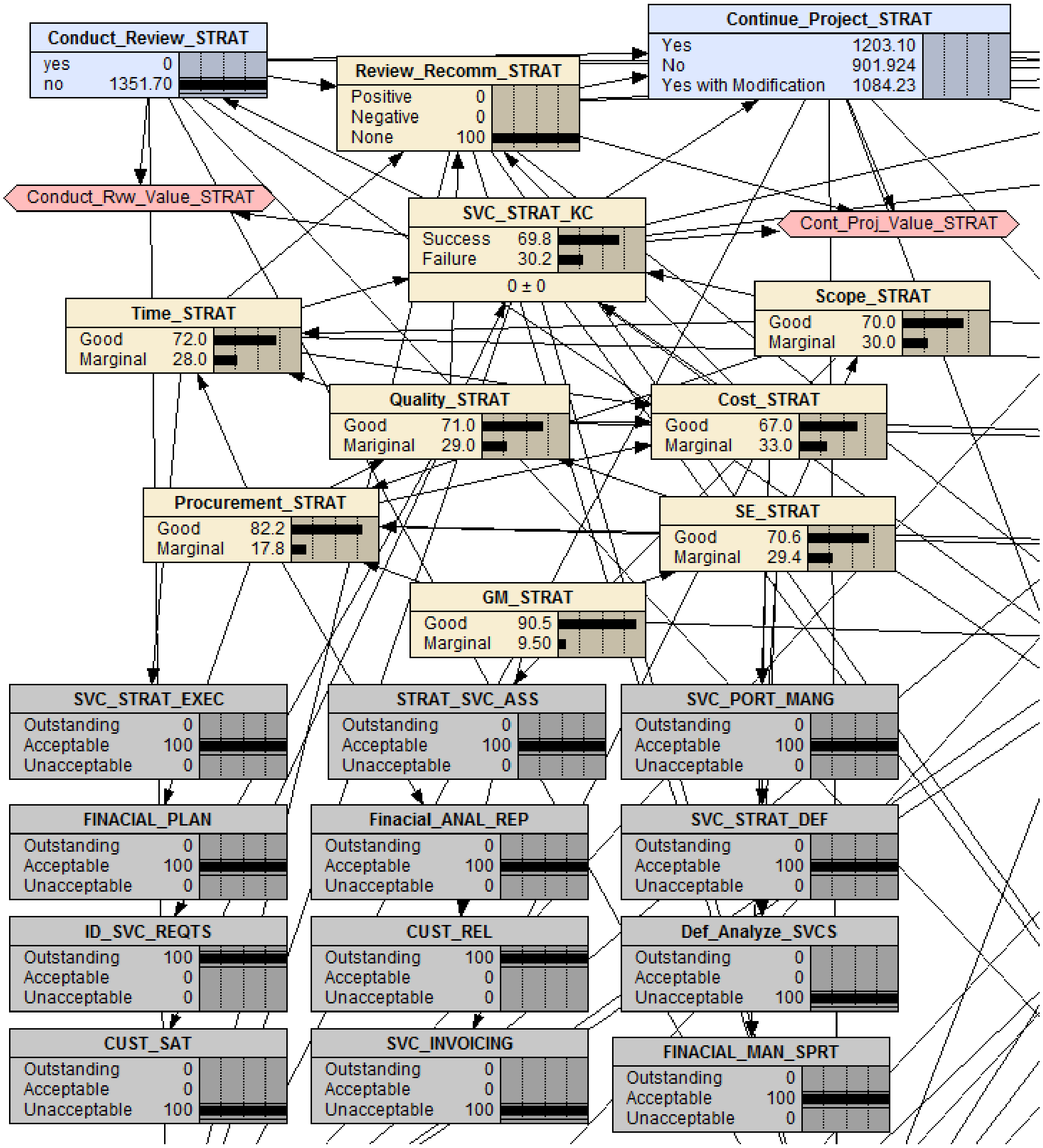


Figure 10. **Service Strategy Scenario Without Program Review**

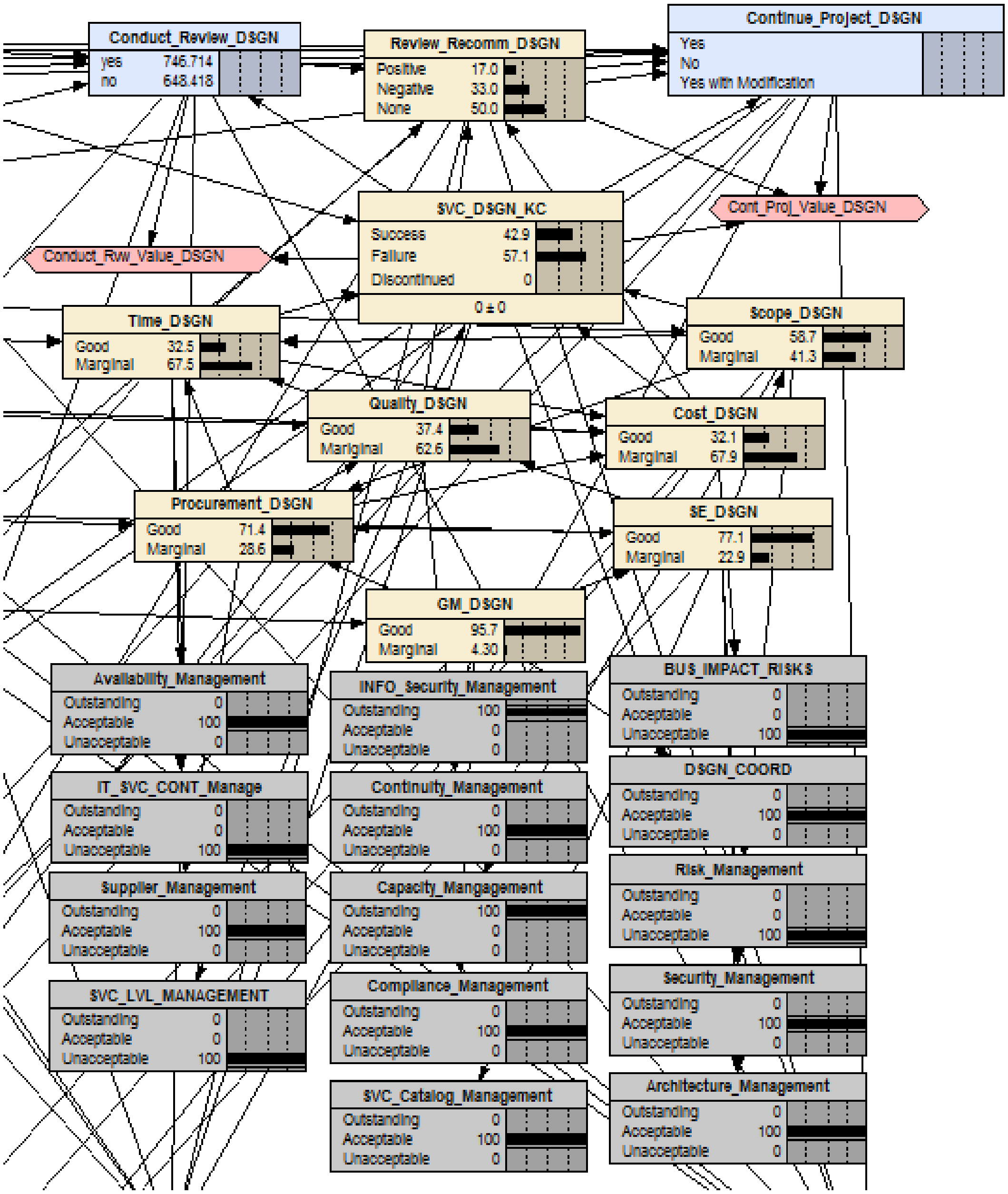


Figure 11. **. ITDMS Service Design Phase With a Failing Program**

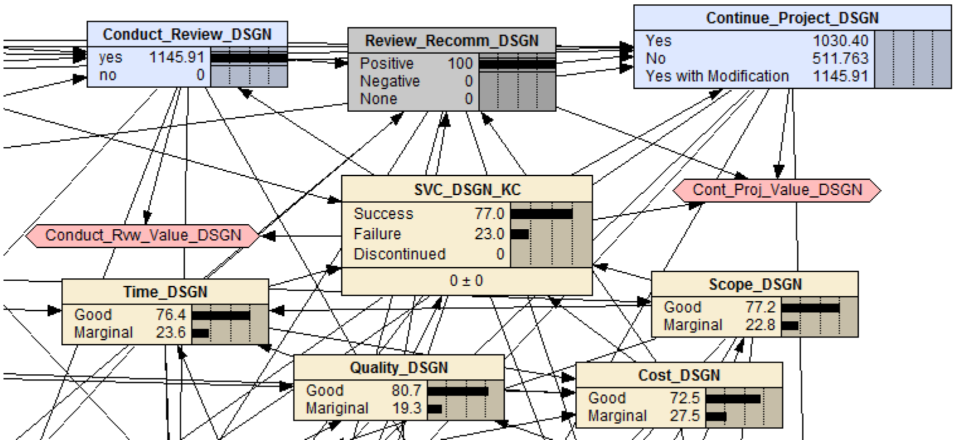


Figure 12. **Service Design Phase Recommendation Given a Satisfactory Review of a Failing Project**

Conclusion and Recommendations

This research developed a potentially useful model/tool to help the systems engineering and IT acquisition professional. Specifically, a quantitative probabilistic reasoning system using BDN to model nonlinear and dynamic relationship within IT acquisition process was developed to gauge program performance and suggest necessary actions. The resulting ITDMS model demonstrates the ability to provide IT managers and decision makers an analytical tool to assess the probability of success with the recommended actions at various points of the project.

The contributions of this research effort include (1) development of a quantitative system to aid decision makers holistically process the available IT acquisition program data and evidence, providing key project success measurement in each of the management areas, and a measurement of success at a review milestone (the knowledge checkpoint); and (2) prediction of future project success with recommended actions through a dynamic Bayesian decision network. The advantage of this approach is its attempt to put the complexity of the ITIL process into a simple model. It is well known, however, that when one is trying to encode a complex problem like the large and highly interconnected one in this study with a simplified model such as a dynamic Bayesian Network, one encounters the trade-off between computational complexity and accuracy.

Future work on the model would be to measure the model with a real-world example of a company or organization using ITIL in their IT service acquisition to determine if it provided correct recommendations. Additionally, a user-friendly interface could be added to the model to enable personnel who are unfamiliar with the Bayesian Network model to input data and receive easily interpreted outputs. Finally, the model is organized for managing an IT system using the ITIL structure from ground-zero to full service implementation. Not all IT acquisitions require the complete ITIL structure and a decision maker may only need to use a few phases of the structure. Therefore, it would be useful to provide a model that is adaptable to the user needs.

References

Agutter, C. (2012). ITIL foundation handbook. London, England: TSO (The Stationery Office).

Bloch, M., Blumberg, S., & Laartz, J. (2012, October). Delivering large-scale IT projects on time, on budget, and on value. Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/delivering-large-scale-it-projects-on-time-on-budget-and-on-value

ClydeBank Technology. (2017). ITIL for beginners: The complete beginner’s guide to ITIL. Albany, NY: Clydebank Media LLC.

Defense Acquisition University. (2003). U.S. Department of Defense extension to a guide to the project management body of knowledge (PMBOK guide). Ft. Belvoir, VA: Defense Acquisition University Press.

Defense Acquisition University. (2013, August). Defense acquisition guidebook. Retrieved from https://dag.dau.mil/Pages/default.aspx

DoD. (2013, November). Operation of the defense acquisition system (Interim DoD Instruction 5000.02). Washington, DC: Author.

Department of Navy. (2012). Naval PoPS guidebook—A program health assessment methodology for Navy and Marine Corps acquisition programs, Version 2.2.

GAO. (2012). DoD financial management (GAO-12-565R). Washington, DC: Author.

GAO. (2015). NASA: Implementing a knowledge- based acquisition framework could lead to better investment decisions and project outcomes (GAO-06-218). Washington, DC: Author.

Gray, J. (2006). The challenges of ITIL implementations. Unpublished master’s thesis, Edith Cowan University. Retrieved from http://ro.ecu.edu.au/theses_hons/1044

Khodakarami, V. (2009, November). Bayesian networks: A novel approach for modelling uncertainty in projects. Retrieved from https://pmiromechapter.files.wordpress.com/2011/05/rome_risksig_conference_vahid_2009.ppt

Laskey, K. (2012, September). Graphical probability models for inference and decision making. Retrieved from http://seor.gmu.edu/~klaskey/GraphicalModels/

Liu, J., Yang, J., & Sii, H. (2002). Review of uncertainty reasoning approaches as guidance for maritime and offshore safety-based assessment. Journal of UK Safety and Reliability Society, 23(1), 63–80.

Neapolitan, R. E. (2004). Learning Bayesian networks. Upper Saddle River, N.J: Prentice Hall.

Netica. (2015). Netica application (Version 4.16) [Computer software]. Retrieved from https://www.norsys.com/netica.html

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD[AT&L]). (2006, August). Risk management guide for DoD acquisition. Washington, DC: Author.

Project Management Institute, Inc. (2008). A guide to the project management body of knowledge (PMBOK Guide) (4th ed.). Newtown Square, PA: Author.

Schum, D. A. (2001). The evidential foundations of probabilistic reasoning. Evanston, IL: Northwestern University Press.

Steven, D. (2014). A measure of systems engineering effectiveness in government acquisition of complex information systems: A Bayesian belief network-based approach (Doctoral dissertation). Washington, DC: The George Washington University.

Taylor, S. (2011). ITIL service strategy. Norwich, England: TSO (The Stationery Office).

Tzeng, S. (2015). Management toward success—Defense business system acquisition probability of success model. Unpublished doctoral dissertation, George Mason University, Washington, DC.

Tzeng, S., & Chang, K. (2015). Management toward success—Utilization of analytics in acquisition decision making. Defense Acquisition Review Journal, 22(2), 192–214.

Yoo, W. S. (2007). An information-based decision making framework for evaluating and forecasting a project cost and completion date (Doctoral dissertation, The Ohio State University).

Zhang, Y., & Ji, Q. (2006). Active and dynamic information fusion for multisensor systems with dynamic Bayesian networks. IEEE Transactions on Systems, Man and Cybernetics, Part B (Cybernetics), 36(2), 467–472. doi:10.1109/tsmcb.2005.859081

Panel 12. Key Challenges in Design and Engineering Management of Programs

Wednesday, May 8, 2019	
3:45 p.m. – 5:00 p.m.	**Chair: Reuben Pitts,** President, Lyceum Consulting, LLC ***Lead Systems Integration: A Key Enabler for System of Systems Engineering and Integration*** Ronald Carlson and Warren Vaneman, Naval Postgraduate School ***Uncovering Cascading Vulnerabilities Within Model-Centric Acquisition Programs and Enterprises*** Donna Rhodes and Jack Reid, Massachusetts Institute of Technology ***Risk Management and Information Assurance Decision Support*** Hanan Hibshi and Travis Breaux, Carnegie Mellon University

Reuben Pitts—is the president of Lyceum Consulting. He joined the Naval Weapons Lab in Dahlgren, VA, in June 1968 after graduating from Mississippi State University with a BSME. His early career was spent in ordnance design and weapons systems. He subsequently served on the planning team to reintroduce the Navy to Wallops Island, VA, currently a multiple ship combat, over-the-water weapons testing lab for Surface Ship Combat Systems, Fighter Aircraft, and live missile firings. His outstanding service as the deployed science advisor to commander, U.S. Sixth Fleet, was recognized with the Navy's Superior Civilian Service (NSCS) Award and the Navy Science Assistance Program Science Advisor of the Year Award.

Pitts was selected to lead the technical analysis team in support of the formal JAG investigation of the downing of Iran Air Flight 655 by USS Vincennes, and participated in subsequent briefings to CENTCOM, the chairman of the joint chiefs, and the secretary of defense. As head, Surface Ship Program Office and Aegis program manager, Pitts was awarded a second NSCS, the James Colvard Award, and the John Adolphus Dahlgren Award (Dahlgren's highest honor) for his achievements in the fields of science, engineering, and management. Anticipating the future course of combatant surface ships, Pitts co-founded the NSWCDD Advanced Computing Technology effort, which eventually became the Aegis/DARPA-sponsored High Performance Distributed Computing Program, the world's most advanced distributed real-time computing technology effort. That effort was the foundation for the Navy's current Open Architecture Initiative. In 2003, Pitts accepted responsibility as technical director for PEO Integrated Warfare Systems (IWS), the overall technical authority for the PEO. In September of that year, he was reassigned as the major program manager for Integrated Combat Systems in the PEO. In this position, he was the program manager for the Combat Systems and Training Systems for all U.S. Navy Surface Combatants, including aircraft carriers, cruisers, destroyers, frigates, amphibious ships, and auxiliaries. In July 2006, Pitts returned to NSWCDD to form and head the Warfare Systems Department. While in this position, he maintained his personal technical involvement as the certification official for Surface Navy Combat Systems. He also served as chair of the Combat System Configuration Control Board and chair of the Mission Readiness Review for Operation Burnt Frost, the killing of inoperative satellite USA 193.

Pitts has been a guest speaker/lecturer/symposium panelist at many NAVSEA-level and DoD symposiums and conferences and at the Naval Postgraduate School, the Defense Systems Management College, and the National Defense University. For 19 years, Pitts was the sole certification authority of all Aegis Combat System computer programs for fleet use. He retired from the U.S. Civil Service in September 2008, with over 40 years of service to the Navy.

Lead Systems Integration: A Key Enabler for System of Systems Engineering and Integration

Ronald R. Carlson—served 26 years in naval aviation as a pilot, seven years of which were at NAVAIR where he led NAVAIR Systems Engineers through several years of systems engineering revitalization. He joined the NPS SE department nine years ago. He has a Master of Philosophy from Stevens Institute of Technology, master's degrees in strategic studies and national policy from the Naval War College and business administration–aviation from Embry Riddle Aeronautical University, and a Bachelor of Science in nuclear engineering from the University of Michigan. [rrcarlso@nps.edu]

Warren Vaneman—has more than 32 years of leadership and systems engineering experience from various positions within the intelligence community, including as Chief Architect of the Enterprise Ground Architecture at the National Reconnaissance Office. He is also a Retired Navy Reserve Captain. He has a BS from the State University of New York Maritime College, an MS in systems engineering and PhD in industrial and systems engineering from Virginia Tech, and a Joint Professional Military Education Phase 1 Certificate from the Naval War College. The International Council on Systems Engineering (INCOSE) certifies him as a Certified Systems Engineering Professional (CSEP). [wvaneman@nps.edu]

Abstract

Lead Systems Integration (LSI) is an acquisition strategy that employs a series of methods, practices, and principles to increase the span of both management and engineering acquisition authority and control to acquire a System of Systems (SoS) or highly complex systems. LSI is effectively a "marriage" of program management and multiple functional disciplines which must work together cooperatively to assert and execute trade space in the SoS given multiple constituent system acquisitions. To successfully plan, develop, and manage an SoS, a comprehensive development, acquisition, and implementation strategy is required. Our previous research defined the LSI Enterprise Framework as a means to engineer and manage the capabilities and interdependencies of an SoS, that can be executed by the government LSI, across multiple systems, programs, and stakeholder levels. This paper highlights the results from our Fiscal Year 2018 Acquisition Research Program effort. It discusses the integration of the LSI with other processes, used by Navy System Commands (SYSCOMs), to engineer and manage SoS, and provides a blueprint for a more complete governance approach.

Introduction

> *We need … to seek creative solutions to today's and tomorrow's complex problems. … We need to change where it makes sense, adapt as quickly as possible, and constantly innovate to stay ahead of our adversaries. Our ability to adapt more quickly than our enemies will be vital to our future success.* —General R.B. Neller, USMC (2016)

To stay ahead of our adversaries, the military must improve the capability of its systems. These systems are becoming increasingly complex, and so has the effort to develop them. To achieve the improved capabilities, gaps/shortfalls in systems are being filled by integrating them with other systems that possess the required capability. Some of these systems are legacy systems, some are new systems, and some are systems still under development. Furthermore, these systems do not just need to be integrated, they need to be interoperable. They need to speak the same language, use the same units, and if more than one system can sense the same things, they need to determine which data is more accurate.

In the early 2000s, a few high visibility government projects were failing. They were strongly criticized because of cost and schedule overruns, and apparent conflicts of interest. There were multiple contributing factors in these failures: SE practices were not adequate to define and manage these complex programs, they were producing unprecedented System of Systems (SoS) with constituent systems that were in various levels of development, and government procurement policies changed in the 1990s. Additionally, the government did not have the necessary visibility into these projects to foresee impending problems because contractors were performing the design and integration work. These contracted systems integrators often re-allocated resources or funding between disparate programs/program offices or even chose which programs (or contractors) would be used. This led to numerous potential conflicts of interest as well as a loss of control and oversight by the government.

The acquisition and management of mission capabilities across the SoS lifecycle require the complex integration of interdependent new and legacy systems from the lowest component level to the highest enterprise level. The challenge of integrating these disparate constituent systems into an SoS is that they are developed and procured asynchronously, usually by different program offices, and often across different enterprises.

Heretofore, Navy System Commands (SYSCOMs) have been using different approaches to address SoS issues. The two most prevelant approaches are Lead Systems Integration (LSI) and Navy Integration and Interoperability (I&I). LSI is an acquisition strategy that employs a series of methods, practices, and principles to increase the span of both management and engineering acquisition authority and control to acquire an SoS or highly complex systems. The Navy I&I provides an SoS and governance process to identify gaps in Naval missions and to develop and coordinate solutions across system boundaries. Navy I&I provides a more detailed strategy than LSI, but is focused primarily on the early phases of the SoS lifecycle. LSI is more broadly defined, but lacks the details sufficient for an implementation strategy that can be used across the SoS lifecycle. Each of these processes provide clarity to a portion of the challenges faced by government personnel conducting complex SoS integration. However, none stands alone as a prescriptive document to enable the full spectrum of activities required to engineer and manage an SoS.

Both LSI and Navy I&I have a common foundation: the System of Systems Engineering and Integration (SoSE&I) "Vee." The SoSE&I "Vee" provides a model of the high-level activities that need to be performed in engineering and management throughout the SoS lifecycle, but fails to provide implementation guidance, and equally important, it doesn't suggest who performs these activities. Neither LSI or Navy I&I address the full spectrum of the problem. However, LSI provides the broadest framework to address the SoSE&I "Vee." Given that the LSI Enterprise Framework offers the broadest perspective, further defining and enhancing, LSI activities using the SoSE&I "Vee" as the foundation, was used as the premise of this research.

This paper highlights the results from our Fiscal Year 2018 Acquisition Research Program effort. It discusses the integration of the LSI and I&I processes with the SoSE&I "Vee," and establishes the foundation that provides a blueprint for a more complete SoS governance approach. The revised process model includes inputs, outputs, and guiding principles of each phase to yield an implementable solution that can be employed throughout the SoS lifecycle.

Existing System of Systems Processes

This research considered the two previously mentioned strategies in relation to the SoSE&I "Vee" to address the Navy's overall problem with LSI. Systems and SoS are becoming more complex, and emerging threats are proving themselves to be more pressing. As a result, a critical need for integrated and interconnected systems has emerged. The implementation of SoSE&I using LSI techniques must be developed to adequately influence the ever-increasing complexity of the national defense enterprise.

System of Systems Engineering and Integration "Vee"

Essential to the understanding of this research is an understanding of the SoSE&I "Vee." An SoS is "a set or arrangement of systems that results when independent and task-oriented systems are integrated into a larger system that delivers unique capabilities" (Vaneman & Budka, 2013, p. 2). Further defining an SoS is the attribute where the whole is greater than the sum of its parts (Office of the Deputy Under Secretary of Defense (Acquisition and Technology), Systems and Software Engineering [ODUSD(A&T)SSE], 2008). SoSE&I incorporates the basic tenants of SE within the SoS framework and results in "planning, analyzing, organizing, and integrating the capabilities of a mix of existing and new constituent systems into an SoS capability greater than the sum of the capabilities of the constituent systems" (Vaneman, 2016). SoSE&I thus becomes the framework of choice for solving tomorrow's problems as they relate to pressing and emerging threats to the United States. The SoS approach to national defense provides the structure to develop new capabilities through the integration of new and constituent systems. A common foundation for delivering these complex systems is captured in the SoSE&I "Vee," which has built upon the traditional SE "Vee."

The SoSE&I "Vee" is depicted in Figure 1 (Vaneman, 2016). This high-level depiction of the SoSE&I "Vee" provides useful context in using the overall SoS architecture for performing top-down engineering (as in traditional SE) and performing bottom-up verification and validation.

The SoSE&I "Vee" begins at the upper-left side with SoS Architecture & Requirements Development. In this phase, the user needs are defined and transformed into technical requirements that can be executed by the system program office (Vaneman, 2016). The purpose of Architecture and Requirements Development is not only to understand the overall mission needs and establish the boundary of the SoS of interest, but also to uncover the requirements for the individual constituent systems needed to achieve the mission capabilities, their respective interfaces, and to manage and implement SoSE&I processes. It is equally important to develop a comprehensive plan to align systems that are meant to work together for mission success, provide a foundation from which resources can be prioritized to maximize user needs and budget issues, and establish an overarching requirements baseline to improve integration and interoperability across the SoS (Vaneman, 2017).

The bottom of the SoSE&I "Vee" represents the systems engineering activities that are performed by the program offices of the constituent systems. Several individual system SE "Vees" are depicted to illustrate that many constituent systems are developed and managed concurrently, with each system at different maturity levels within its own lifecycle. In this phase, the focus is on the development, sustainment, and management of individual systems (Vaneman, 2016).

The upper-right side of the SoSE&I "Vee" represents the SoS Mission Assurance activities. Mission Assurance is defined as "the part of systems engineering and integration activities which, by means of a combination of design validation, product verification, and systems test, provides the systems engineers, design team, and customer with a high degree of confidence in the successful execution of the required system functions" (Guarro, 2007, p. 14). More plainly, as one moves along the right side of the SoSE&I "Vee," the Mission Assurance process ensures SoS success is documented in the context of mission success from the integration of systems to the operations and sustainment of the SoS. If individual systems meet their individual requirements but SoS interoperability and certification are not achieved, a reassessment of the requirements that were flowed down to the constituent systems is required to be performed in order to ensure individual capabilities combine to provide a more useful SoS capability. Similarly, if the SoS performs adequately but is unsupportable or unsustainable, its requirements will need to be reassessed. Another critical step in this process is the integration of the SoS's constituent systems.

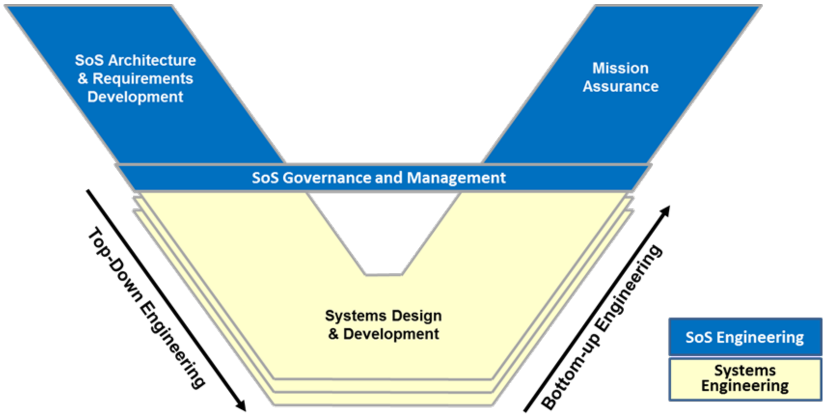

SoS Architecture & Requirements Development
Mission Assurance
SoS Governance and Management
Top-Down Engineering
Systems Design & Development
Bottom-up Engineering
SoS Engineering
Systems Engineering

Figure 1. **The SoSE&I "Vee"**

The final component of the SoSE&I "Vee" is SoS Governance and Management. While not formally described as a process, Governance and Management is a cornerstone of an effective SoS and is comprised of the set of rules, policies, and decision-making criteria that will guide the SoS team to achieve its goals and objectives (Vaneman, 2016). As the complexity of modern SoS increases, the multitude of technical and managerial activities involved become more entangled. As a result, a strong SoS governance and management approach is imperative to address complex emergent issues and those directly related to the triple constraint of cost, schedule, and performance.

The Lead Systems Integration Enterprise Framework

As stated earlier, Lead Systems Integration is an acquisition strategy that employs a series of methods, practices, and principles to increase the span of both management and engineering acquisition authority and control to acquire an SoS or highly complex systems. The LSI function is to assert and execute SoS and stakeholder trade space to affordably optimize integrated mission capabilities across the SoS lifecycle (NPS LSI Cohort #1, 2014). The roles of the LSI are similar to the roles of any systems engineer or system integrator within a program office. The primary difference is the span of LSI design and integration authority that persists throughout the SoS lifecycle (Vaneman & Carlson, 2017).

The LSI Enterprise Framework defines a means to engineer and manage the capabilities and interdependencies of an SoS that can be executed by the government LSI, across multiple systems, programs, and stakeholder levels. The LSI Enterprise Framework (hereafter known as the LSI Framework) captures the complex, interdependent, and mission capability areas through four enterprise levels to characterize the systems from the enterprise to the component level (NPS LSI Cohort #2, 2015; Vaneman & Carlson, 2017). Figure 2 (NPS LSI Cohort #2, 2015) depicts the LSI Enterprise Framework. This framework allows for the alignment of key LSI activities across the enterprise by aligning appropriate touchpoints to the various LSI levels and tasks.

The foundation of the LSI Framework are the four LSI levels. The Enterprise Level is the top layer of the LSI Framework that consists of a variety of stakeholders, from one or many organizations that represent the complex, socio-technical systems that comprises interdependent resources of people, information, and systems that must interact with each other and their environments to achieve mission success (Giachetti, 2010). It is at this level where the capabilities required to achieve enterprise mission success are defined, decomposed into mission capabilities, and allocated to the SoS level to be satisfied as mission capabilities (Vaneman & Carlson, 2018). While the majority of the LSI engineering and management activities occur below the enterprise level, this level is important because this is where organizational, policy, and resource decisions are made for the LSI (Vaneman & Carlson, 2018).

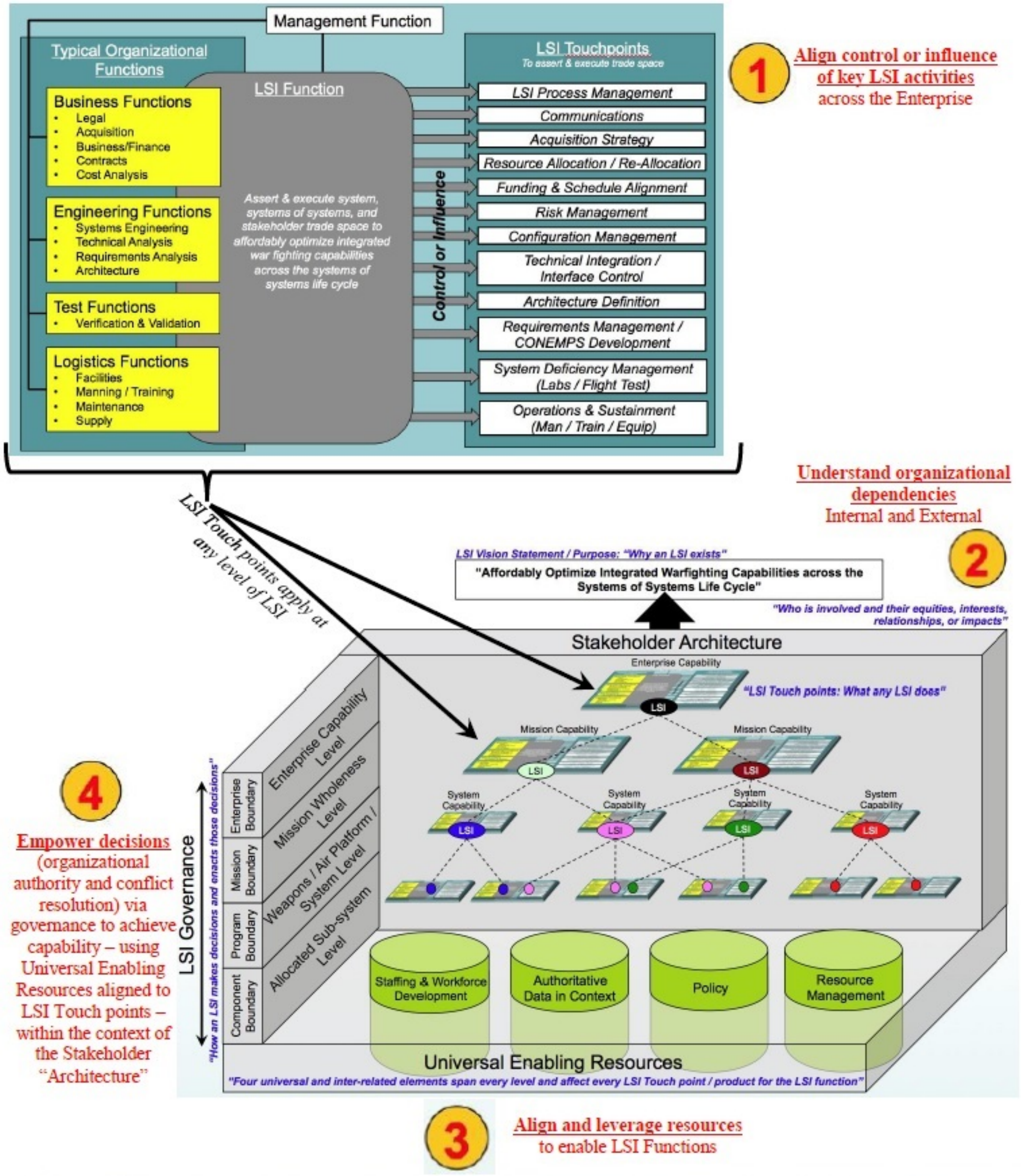

Management Function
Typical Organizational Functions
Business Functions
• Legal
• Acquisition
• Business/Finance
• Contracts
• Cost Analysis
Engineering Functions
• Systems Engineering
• Technical Analysis
• Requirements Analysis
• Architecture
Test Functions
• Verification & Validation
Logistics Functions
• Facilities
• Manning / Training
• Maintenance
• Supply
LSI Function
Assert & execute system, systems of systems, and stakeholder trade space to affordably optimize integrated war fighting capabilities across the systems of systems life cycle
Control or Influence
LSI Touchpoints
To assert & execute trade space
LSI Process Management
Communications
Acquisition Strategy
Resource Allocation / Re-Allocation
Funding & Schedule Alignment
Risk Management
Configuration Management
Technical Integration / Interface Control
Architecture Definition
Requirements Management / CONEMPS Development
System Deficiency Management (Labs / Flight Test)
Operations & Sustainment (Man / Train / Equip)
1
Align control or influence of key LSI activities across the Enterprise
LSI Touch points apply at any level of LSI
Understand organizational dependencies
Internal and External
2
LSI Vision Statement / Purpose: "Why an LSI exists"
"Affordably Optimize Integrated Warfighting Capabilities across the Systems of Systems Life Cycle"
"Who is involved and their equities, interests, relationships, or impacts"
Stakeholder Architecture
Enterprise Capability
"LSI Touch points: What any LSI does"
LSI
Mission Capability
Mission Capability
System Capability
System Capability
System Capability
System Capability
Enterprise Capability Level
Mission Wholeness Level
Weapons / Air Platform / System Level
Allocated Sub-system Level
Enterprise Boundary
Mission Boundary
Program Boundary
Component Boundary
LSI Governance
"How an LSI makes decisions and enacts those decisions"
4
Empower decisions (organizational authority and conflict resolution) via governance to achieve capability – using Universal Enabling Resources aligned to LSI Touch points – within the context of the Stakeholder "Architecture"
Staffing & Workforce Development
Authoritative Data in Context
Policy
Resource Management
Universal Enabling Resources
"Four universal and inter-related elements span every level and affect every LSI Touch point / product for the LSI function"
3
Align and leverage resources to enable LSI Functions

Figure 2. **Lead System Integration Enterprise Framework**

The Mission Wholeness Level is where a collection of supporting constituent systems and programs are brought together to support end-to-end capability effectiveness for the designated mission areas. Accomplishing a mission that cannot be satisfied by a single system alone has always been an SoS endeavor, but integrating the multiple systems together has frequently been left to small communities consisting of a few systems or the operators themselves (Department of the Navy, 2013). Many LSI governing efforts, at the System of Systems Level, involve a collaborative partnership of multiple program offices, versus a more directive effort that may occur at lower program levels (NPS LSI Cohort #1, 2015). Individual capabilities and functions are allocated to constituent systems for implementation (Vaneman & Carlson, 2018).

The System Level is where a combination of functionally related physical elements are integrated into a usable, system to achieve the system capability. In this level, the emphasis is on traditional systems engineering and development activities. However, two significant roles are important to the LSI. First, the LSI must ensure that the SoS level organization has sufficient insight into the individual programs within the SoS to understand the functionality and interoperability that will result from the engineering and design effort. Second, the LSI must ensure a strong governance model is in place that provides the technical authority to govern system baselines so that the system delivered for integration into an SoS meets the requirements that were allocated to it (Vaneman, 2016). In addition to the LSI's role in ensuring system integration to an SoS, an LSI may be used for the engineering and development of a complex system, where the system is composed of major sub-systems, and a large number of interacting components (Vaneman & Carlson, 2018).

The lowest level of the LSI Framework is the subsystem/component level. This level consists of the allocated sub-systems and components that by themselves may, or may not, provide a usable standalone end product. These are the lowest level building blocks required for any LSI effort and may be managed by a team in a larger program office, or may be managed separately by sub-system program offices (NPS LSI Cohort #2, 2015; Vaneman & Carlson, 2018).

Given the breadth of an SoS acquisition effort and recognizing that an LSI's resources to manage an effort are limited, an LSI must be able to efficiently focus on the highest payoff "touchpoints" of control or influence to assert and execute trade space—aligned across the enterprise—to enable organizational agility. Although previous research has discussed inherently governmental functions for an LSI at a high level, there has been unclear specific applicability to current program processes and organizations—and some definitions also did not fully account for multidisciplinary functions that extend beyond systems engineering (NPS LSI Cohort #2, 2015; Vaneman & Carlson, 2017).

The LSI Framework defines 12 key touchpoints (shown in Figure 2) that apply across all domains as the essential "high payoff" functions and activities. These LSI touchpoints are the functions that assert and execute SoS, complex system, and stakeholder trade space to affordably optimize integrated war fighting capabilities across the system of systems lifecycle. These touchpoints do not necessarily define new processes, but do identify how existing processes can be enhanced and used more efficiently (NPS LSI Cohort #2, 2015). For a detailed discussion of the LSI touchpoint see Vaneman and Carlson (2017).

Universal enabling resources—staffing and workforce development, policies, resource management, and the authoritative data context—are those resources that support LSI-unique execution at any of the touchpoints to assert and execute the trade space. These four enabling resources and inter-related enablers apply at all levels in the LSI Enterprise Framework, and are outside the responsibilities of the typical program offices.

However, the LSI must be aware of these activities, and navigate within them (Carlson & Vaneman, 2018).

Finally, governance empowers decisions across the enterprise by providing a set of decision-making criteria, policies, processes, and actions that guide the stakeholder architecture to achieve the enterprise goals and objectives (Vaneman & Carlson, 2018).

Navy Integration and Interoperability

Navy Integration and Interoperability (I&I) provides SoS and governance processes to identify gaps in naval missions, and to develop and coordinate solutions across system boundaries. To identify the mission gaps, system interaction and behaviors are derived from an enterprise view of naval operational environments and mission objectives (Department of the Navy, 2016). Navy I&I is an important concept to this LSI research because I&I provides detailed processes in the SoS Architecture and Requirements phase of the SoSE&I “Vee” whereas the LSI Framework provides a general overview of the needed processes. These processes together largely focus on the Mission Engineering “Vee,” which is very similar to the SoSE&I “Vee,” and they can easily be extrapolated to SoSE&I. This Integrated Capability Framework (ICF) is shown in Figure 3 (Vaneman & Carlson, 2018).

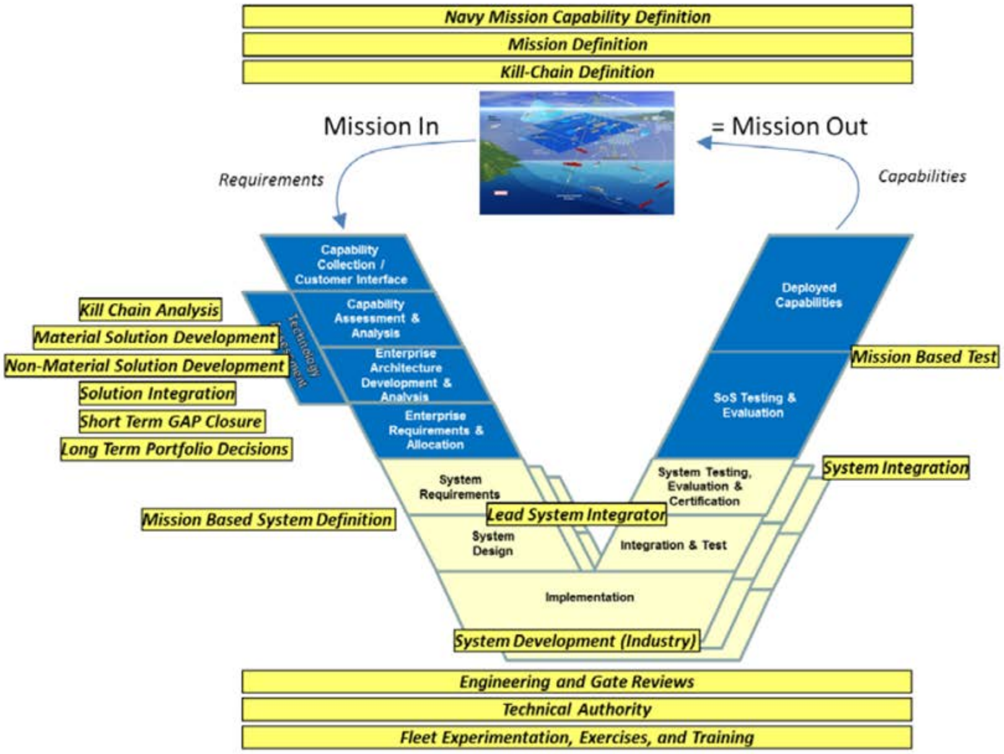

Navy Mission Capability Definition
Mission Definition
Kill-Chain Definition
Mission In
= Mission Out
Requirements
Capabilities
Capability Collection / Customer Interface
Capability Assessment & Analysis
Enterprise Architecture Development & Analysis
Enterprise Requirements & Allocation
Technology Assessment
Kill Chain Analysis
Material Solution Development
Non-Material Solution Development
Solution Integration
Short Term GAP Closure
Long Term Portfolio Decisions
Deployed Capabilities
Mission Based Test
SoS Testing & Evaluation
System Integration
System Requirements
System Testing, Evaluation & Certification
Lead System Integrator
Mission Based System Definition
System Design
Integration & Test
Implementation
System Development (Industry)
Engineering and Gate Reviews
Technical Authority
Fleet Experimentation, Exercises, and Training

Figure 3. **Integrated Capability Framework Use Cases Applied to the SoSE&I “Vee”**

The I&I process begins with a Warfare Capability Baseline (WCB) assessment which “uses the concept of a kill chain to organize, or model, the functions performed in the execution of a mission” (Department of the Navy, 2016, p. 12). The goal of the I&I process is to accomplish four distinct tasks: (i) address materiel gaps identified by the WCB; (ii) build mission-based architectures as a basis for system acquisition; (iii) use I&I decisions as a driver to SE reviews and gate processes; and (iv) share mission related information across Systems Commands (SYSCOMs).

As it relates to the SoSE&I “Vee,” the first step in the I&I process is the definition of the mission needs and requirements. The significance of this important first step is that it establishes the needs for system development of the constituent systems within the SoS. The mission needs and requirements serve as the primary input to the SoS Architecture and Requirements Development portion of the SoSE&I “Vee,” and provide a constant reference for technological progress checks.

Following Mission Definition, I&I establishes the SoS interfaces involved based on the required mission parameters, requirements, and capabilities. This accounts for organizational relationships and helps to define SoS capabilities and needs. The common framework provided by I&I seeks to “facilitate enterprise level engineering across the SYSCOMs and enables efficient system integration and effective force interoperability” (Department of the Navy, 2016, p. 5). This helps lay the ground work needed for individual system design and development.

As can be seen in the ICF, the I&I process is intended to support the warfighter through a mission-based focus on SE, support to the acquisition process by identifying consistent requirements for the SoS early in the process and assisting with analysis efforts through a common I&I repository. Though the I&I process is intended to span the Mission Engineering “Vee” (or SoSE&I “Vee”), it is largely focused on requirements and interface definition and does not provide much SoSE&I detail. As such, the process does not stand on its own.

Use of the ICF enables consistent and more complete definition of Naval warfighter needs, and ensures that all stakeholders from initial concept to test and training understand what the definition of success is for any new or upgraded system. Additionally, training and testing efforts can use the same missions defined in the front end to perform the operational tests and training exercises, ensuring that the systems and sailors are tested and trained in accordance with planned missions. Use of Fleet-defined operational requirements, captured through ICF Mission Models, helps system and platform requirement definition and design, providing a validated and complete mission context including planned operational use during system development. The mission definition also provides system and platform owners with a thorough set of interoperability requirements and ensures existing capabilities are not duplicated. Finally, when completed with operational and system/platform measures tied to mission desired effects, the ICF enables analysis of I&I issues and mission gaps, and the tracking of closure for each one within the SoS (Department of the Navy, 2016).

The Evolution of the LSI Enterprise Framework

Evolving the LSI Enterprise Framework From the SoSE&I “Vee” Model

Lead Systems Integration, and Navy I&I, have emerged as the leading strategies to address SoS issues within the Navy. While each strategy offers insights and partial solutions to the challenges posed by the SoS engineering and acquisition environment, neither addresses the problem that spans the entire SoS lifecycle. One of the goals of this research is to expand the LSI concept by defining an implementation strategy that can be used the across the SoS lifecycle phases and organizational boundaries (Carlson & Vaneman, 2018).

As previoulsy stated, the SoSE&I “Vee” can be used as the common denominator or foundation between LSI and Navy I&I. The LSI Framework represents the process, at a high level, so it can be used to better understand, engineer, and manage the SoS. However, it does not provide the necessary detail for operational use. Navy I&I discusses portions of the SoSE&I “Vee,” in more detail than is offered by the LSI Framework, and could be used to better define the SoS. However, Navy I&I is mostly concerned with the SoS Architecture and

Requirements Development Phase of the SoSE&I "Vee." Essentially, LSI provides the breadth across the SoSE&I phases, while Navy I&I captures the depth of one of those phases.

The four top level functions of the SoSE&I "Vee" are shown in Figure 1. These four functions can be decomposed further to provide additional, actionable detail. The SoSE&I "Vee" model does not include the inputs and outputs for each function, the rules and policies governing the activities, or the skills needed to perform those activities. These elements are needed to fully develop an LSI implementation strategy.

To better understand the SoSE&I functions, each were analyzed for inputs, outputs, controls, and position descriptions. Using the Integrated Definition Function Model (IDEF0), the SoSE&I functions can be expanded to incorporate both the LSI and Navy I&I processes. Figure 4 shows a generic depiction of the IDEF0 model. The functional activities (shown in the box) are represented by the SoSE&I functional activities. The inputs (entering from the left) and outputs (exiting from the right) are represented by the inputs to, and outputs from, each SoSE&I functional activity. The controls (entering from the top) are represented by acquisition policies, the LSI touchpoints, and guidance elements defined in the Navy I&I ICF. The mechanisms (entering from the bottom) represent the SoS acquisition position descriptions (knowledge, skills, and abilities) needed to perform the functional activities (Carlson & Vaneman, 2018).

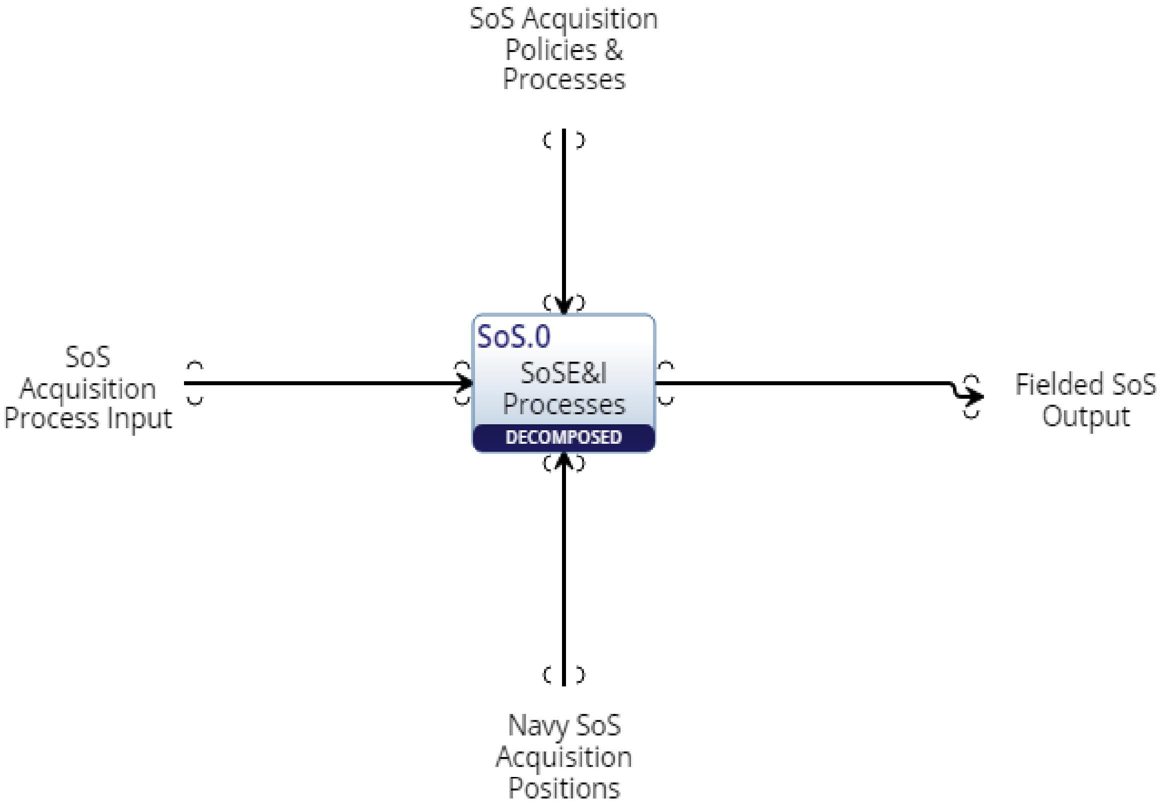

SoS Acquisition Policies & Processes
SoS Acquisition Process Input
SoS.0
SoSE&I Processes
DECOMPOSED
Fielded SoS Output
Navy SoS Acquisition Positions

Figure 4. **SoSE&I IDEF0 (Level 0) Model**

Using the IDEF0 construct, the Navy I&I and LSI processes were analyzed to determine how they may further govern the SoSE&I functions. Figure 5 (Carlson &

Vaneman, 2018) shows the SoSE&I “Vee” as an IDEF0 model. The model illustrates the interdependencies throughout the entire process flow from initial requirements through support of the fielded systems. The correlation between the LSI and I&I processes, embedded on the SoSE&I “Vee,” provides the blueprint for a more complete SoS governance approach with a more executable set of guidelines and should result in an enhanced mission-based SoS development and LSI management effort.

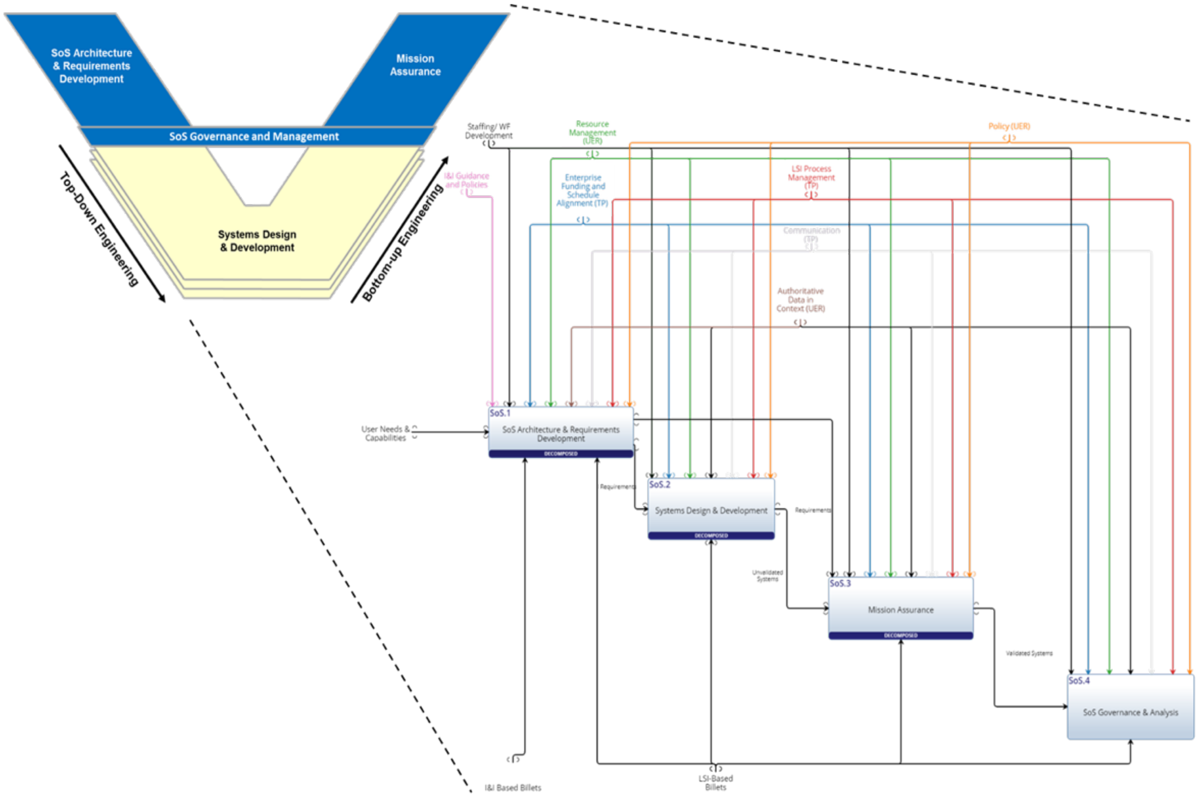

SoS Architecture & Requirements Development
Mission Assurance
SoS Governance and Management
Systems Design & Development
Top-Down Engineering
Bottom-up Engineering
Staffing/ WF Development
Resource Management (UER)
Policy (UER)
I&I Guidance and Policies
Enterprise Funding and Schedule Alignment (TP)
LSI Process Management (TP)
Communication (TP)
Authoritative Data in Context (UER)
User Needs & Capabilities
SoS.1
SoS Architecture & Requirements Development
DECOMPOSED
Requirements
SoS.2
Systems Design & Development
DECOMPOSED
Requirements
Unvalidated Systems
SoS.3
Mission Assurance
DECOMPOSED
Validated Systems
SoS.4
SoS Governance & Analysis
I&I Based Billets
LSI-Based Billets

Figure 5. **Expanding the SoSE&I “Vee” to an IDEF0 Model**

Carlson and Vaneman (2018) further define each of the SoSE&I functions, into subsequent IDEF0 views, to the next level of decomposition. The basis of this further defintion is the decomposed SoSE&I “Vee” model (Vaneman & Budka, 2013; Vaneman, 2016). The entire decomposition of the SoSE&I “Vee,” and subsequesnt development of the corresponding IDEF0 views is beyond the scope of this paper.

For illustration purposes, the decomposition of the SoS Architecture and Requirements Development function is discussed next. (The interested reader can find details of these decomposed SoSE&I functions in Vaneman and Budka, 2013; Vaneman, 2016; and Carlson and Vaneman, 2018.)

SoS Architecture and Requirements Development

The SoSE&I “Vee” begins at the upper-left side with SoS Architecture & Requirements Development. In this phase the user needs are defined, and then transformed into technical requirements that can be executed by the system program office (Vaneman, 2016). The purpose of Architecture and Requirements Development is not only to understand the overall mission needs, and establish the boundary of the SoS of interest, but also to uncover the requirements for the individual constituent systems needed to achieve the mission capabilities, their respective interfaces, and to manage and implement SoSE&I processes. It is equally important to develop a comprehensive plan to align systems that are meant to work together for mission success, provide a foundation from which resources can be prioritized to maximize user needs and budget issues, and establish an overarching requirements baseline to improve integration and interoperability across the SoS (Vaneman, 2017).

The decomposition of the SoS Architecture and Requirements Development stage, as depicted in Figure 6 (Vaneman & Carslon, 2018), relies heavily on existing I&I and LSI processes to provide the guiding principles, or controls. When depicted in this fashion it is clear that neither the existing I&I processes nor LSI Touchpoints covered the entirety of this phase. However, once combined, a more complete process begins to emerge.

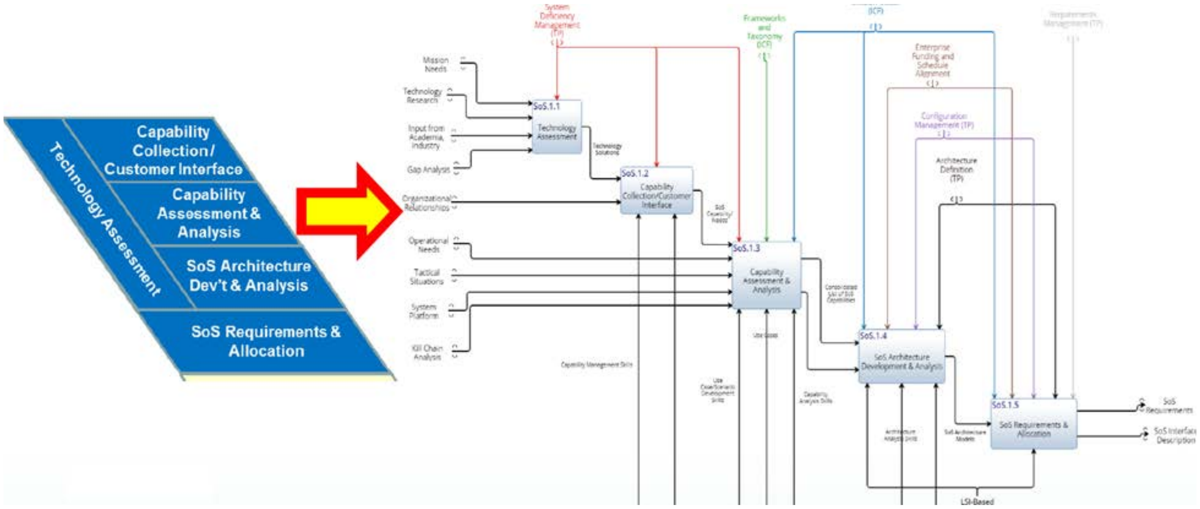

Technology Assessment
Capability Collection / Customer Interface
Capability Assessment & Analysis
SoS Architecture Dev't & Analysis
SoS Requirements & Allocation
System Deficiency Management (TP)
Frameworks and Taxonomy (ICF)
(ICF)
Requirements Management (TP)
Enterprise Funding and Schedule Alignment
Configuration Management (TP)
Architecture Definition (TP)
Mission Needs
Technology Research
Input from Academia, Industry
Gap Analysis
Organizational Relationships
Operational Needs
Tactical Situations
System Platform
Kill Chain Analysis
SoS.1.1
Technology Assessment
Technology Solutions
SoS.1.2
Capability Collection/Customer Interface
SoS Capability Needs
SoS.1.3
Capability Assessment & Analysis
Consolidated List of SoS Capabilities
Use Cases
SoS.1.4
SoS Architecture Development & Analysis
SoS.1.5
SoS Requirements & Allocation
SoS Requirements
SoS Interface Description
Capability Management Skills
Use Case/Scenario Development Skills
Capability Analysis Skills
Architecture Analysis Skills
SoS Architecture Models
LSI-Based

Figure 6. **SoS Architecture and Requirements Development Phase**

Conclusion

Lead Systems Integration seeks to reduce risk in the affordable optimization of integrated warfighting capability acquisition efforts across the SoS lifecycle, and to increase the speed of capability delivery to the warfighter. It can be executed within existing organizations via enhancements to legacy processes, methods, and practices if the workforce is trained and motivated to think and act differently. The LSI Enterprise Framework provides an effective set of tools, resources, and concepts to help incrementally incentivize this cultural evolution.

To achieve this goal, the Navy should increase systems engineering and SoSE&I technical and management depth and breadth across the workforce by hiring professionals trained in advanced systems engineering concepts. Additionally, the adoption of a directed universal approach to SoS management, such as that presented in this report, should be implemented across the Navy Enterprise in order for LSI to be truly successful. Not only are well-trained personnel required to ensure success, but top-down directed guidance that is common to all Naval Systems Commands for LSI in SoS will enable this approach.

Additionally, a directed universal approach to SoS management, such as that presented in this report, should be implemented and enforced across the Navy Enterprise in order for LSI to be truly successful. Not only are well-trained personnel required to ensure success, but top-down directed guidance that is common to all naval SYSCOMs for LSI in SoS will enable this approach.

References

Carlson, R., & Vaneman, W. K. (2018). Managing complex systems engineering and acquisition through lead systems integration. In *Proceedings of the 15th Annual Acquisition Research Symposium*. Retrieved from http://www.researchsymposium.org

Department of the Navy. (2013). *Naval system of systems engineering guidebook*. Washington, DC: Author.

Department of the Navy. (2016, February 22). *Navy integration and interoperability (I&I) integrated capability framework (ICF) operational concept document (Version 3.2)*. Unpublished document.

Giachetti, R. (2010). *Design of enterprise systems*. Boca Raton, FL: CRC Press.

Guarro, S. (2007, Fall). The mission assurance guide: System validation and verification achieve success. *Crosslink, 8*(2). Retrieved from http://aerospace.wpengine.netdna-cdn.com/wp-content/uploads/crosslink/V8N2.pdf.

Herdlick, B. (2011). *Establishing an operational context for early system-of-systems engineering activities*. Retrieved from https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2011/system/12968_HerdlickThursday.pdf.

Naval Postgraduate School Lead Systems Integrator (NPS LSI) Cohort #1. (2014, September 25). *The roles of the government-led lead system integrator (LSI).* Unpublished report.

Naval Postgraduate School Lead Systems Integrator (NPS LSI) Cohort #2. (2015, October 2). *An enterprise lead systems integration (LSI) framework*. Unpublished report.

Neller, R. B. (2016). *The Marine Corps operating concept*. Washington, DC: U.S. Marine Corps.

Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering (ODUSD[A&T]SSE). (2008). *Systems engineering guide for systems of systems, Version 1.0.* Washington, DC: Author. Retrieved from https://www.acq.osd.mil/se/docs/se-guide-for-sos.pdf

Vaneman, W. K. (2016). The system of system engineering and integration "Vee" model. In *Proceedings of the 10th Annual IEEE Systems Conference*. IEEE.

Vaneman, W. K., & Budka, R. (2013). Defining a system of systems engineering and integration approach to address the Navy's information technology technical authority. In *Proceedings of the INCOSE International Symposium*. San Diego, CA: INCOSE.

Vaneman, W. K., & Carlson, R. (2017). Defining an enterprise lead system integration (LSI) framework. In *Proceedings of the 12th Annual System of Systems Engineering Conference*. IEEE.

Vaneman, W. K., & Carlson, R. (2018). *Managing complex systems engineering and acquisition through lead systems integration* (NPA-AM-19-008). Monterey, CA: Naval Postgraduate School, Acquisition Research Program.

Uncovering Cascading Vulnerabilities in Model-Centric Acquisition Programs and Enterprises

Donna H. Rhodes—is a principal research scientist at the Massachusetts Institute of Technology, and director of the Systems Engineering Advancement Research Initiative (SEAri). She conducts research on human-model interaction, model curation, model-centric decision making, and innovative approaches for enterprise transformation under the digital paradigm. Previously, she held senior management positions at IBM, Lockheed Martin, and Lucent. Rhodes is a Past President and Fellow of the International Council on Systems Engineering (INCOSE) and an INCOSE Founders Award recipient. She received her PhD in Systems Science from T. J. Watson School of Engineering at Binghamton University. [rhodes@mit.edu]

Jack Reid—is a graduate student with the Space Enabled Research Group at the Massachusetts Institute of Technology. Reid is currently a doctoral student at MIT with research interests concerning the design and management of complex sociotechnical systems, particularly with regard to the anticipation of emergent and cascading behavior. While a master's student, he was a research assistant in the Systems Engineering Advancement Research Initiative (SEAri), performing research on vulnerability assessment methods, model-centric enterprises, and complexity and emergence. He received an MS in both Aeronautics & Astronautics and Technology & Policy at MIT. [jackreid@mit.edu]

Abstract

Digital engineering changes how systems are acquired and developed through the use of model-centric practices and toolsets. Enterprises face new challenges in this transformation, including potential for emergent vulnerabilities within digital engineering environments. While vulnerability analysis of products and systems is standard practice, examining vulnerabilities within the enterprise itself is less common. This research is responsive to the imperatives of the newly released DoD Digital Engineering Strategy that calls for enterprises to mitigate cyber risks and secure digital engineering environments against attacks from internal and external threats, mitigate known vulnerabilities that present high risk to DoD networks and data, and to mitigate risk posed by collaboration and access to vast amount of information in models. This paper presents progress on the ongoing research that focuses on uncovering cascading vulnerabilities as related to digital engineering practice and supporting environments, with special focus on cybersecurity-related vulnerabilities. The approach uses Cause-Effect Mapping (CEM) as a mechanism for better enabling program leaders to anticipate and respond to vulnerabilities within the enterprise. The current investigation is examining enterprise-level vulnerabilities and investigating potential interventions.

Introduction

Vulnerability assessment of products and systems has been actively investigated in recent years, resulting in a family of useful techniques now commonly accepted as good practice (LeSaint, Reed, & Popick, 2015). The assessment of vulnerabilities within the enterprises performing engineering has received relatively little attention. While many of the existing techniques for systems vulnerability assessment will still be useful, some adaptation and additional techniques are necessary. The urgency of investigating this has increased as a result of digital engineering transformation as it changes how systems are acquired and developed through the use of model-centric engineering practices and new types of environments within the enterprise.

Ongoing research has investigated the use of Cause-Effect Mapping as a mechanism for better enabling program leaders to anticipate and respond to vulnerabilities as related to model-centric enterprises and their enabling environments (Mekdeci et al., 2012; Rovito & Rhodes, 2016; Reid & Rhodes, 2018b). A Reference Cause-Effect Map (CEM) for model-centric enterprises resulting from the work to date shows promise for considering the cascading vulnerabilities and potential intervention options. In the continuing investigation, the Reference CEM and other analytic techniques are being further developed and evaluated. Intervention approaches are being identified and mapped to cascading vulnerability chains, providing options for mitigation.

Background

Background is provided in the following subsections to characterize digital engineering and model-centric enterprises. Prior research papers (Reid & Rhodes, 2018a, 2018b) provide additional background information.

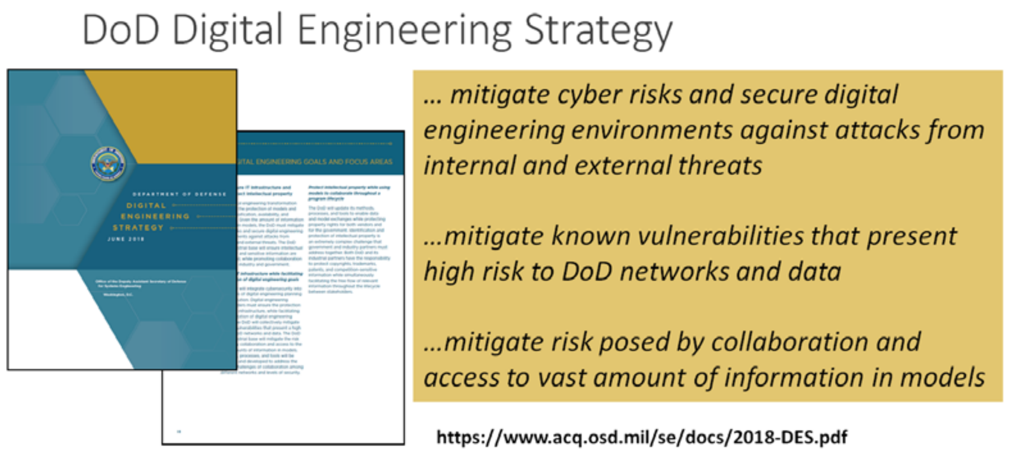
Digital Engineering (Model-Centric Engineering)

Digital engineering (sometimes referred to as model-centric engineering) involves using integrated models across disciplines, subsystems, lifecycle stages, and analyst groups. It uses models as “authoritative source of truth,” to reduce document handoff and allow for more continuous evaluation. By collaborating through models, there is reduced communication time and rework in response to requirement changes. Most discussions to date focus on engineering practices and methods to overcome implementation difficulties. In any system, however, non-technical factors (human factors, business, and organizational) influence engineering effectiveness and model-centric decisions (Reid & Rhodes, 2017; German & Rhodes, 2017).

Current program leaders have significant experience with processes for acquiring and developing systems, and use this experience to identify and mitigate vulnerabilities. Limited experience exists with digital engineering practice and model-centric supporting environments, however. This situation, coupled with the increased model integration and model longevity, means that emergent uncertainties (policy change, budget cuts, disruptive technologies, threats, changing demographics, etc.) and related programmatic decisions (e.g., staff cuts, reduced training hours) may lead to cascading vulnerabilities within digital engineering enterprises, potentially jeopardizing program success. New practices and enablers are needed to assist program leaders in identifying vulnerabilities within the digital engineering environment, and to determine where interventions can most effectively be taken.

Model-Centric Environments

Model-centric environments have many elements, including computing infrastructure, networks, software tools, models, data sets, data storage, and human actors. These environments may come under attack from internal and/or external threats. Some of these elements exist in traditional engineering, but some are new or changed under digital engineering practice (Reid & Rhodes, 2016). New modes of collaboration through models and data are emerging. The quantity of and types of models, digital artifacts, and data has greatly increased. Collaboration between the many enterprises involved through digital engineering (government agencies, contractors, suppliers, etc.) results in significant increases in data flowing across networks. As new toolsets are introduced into enterprise, there are potential risks related to how proficient the workforce is in using these tools and whether there are sufficient controls in place in the management of the digital artifacts produced, as well as the overall supporting infrastructure. The DoD Digital Engineering Strategy (2018) calls for the mitigation of these risks and vulnerabilities (Figure 1).



DoD Digital Engineering Strategy

… mitigate cyber risks and secure digital engineering environments against attacks from internal and external threats

…mitigate known vulnerabilities that present high risk to DoD networks and data

…mitigate risk posed by collaboration and access to vast amount of information in models

https://www.acq.osd.mil/se/docs/2018-DES.pdf

Figure 1. **DoD Digital Engineering Strategy Calls for Mitigation of Risks and Vulnerabilities**

(DoD, 2018)

Vulnerabilities as Causal Chains

Vulnerabilities are effectively expressed as the causal series of events connecting a hazard to the system and/or failure that results. Cause-Effect Mapping is a vulnerability assessment approach that consists of a mapping of causal chains that connect an exogenous hazard to a system degradation or failure, termed a terminal event (Mekdeci et al., 2012). Terminal events are broadly defined and include any form of value loss. A casual chain can be defined as a series of events, with each event causing or being an integral part of the cause, or the next link in the chain. A hazard (spontaneous event) is a system or environmental state that has the potential to disrupt the system. A vulnerability is defined as causal means by which one or more hazards results in the system disruption/value loss. Accordingly, a vulnerability chain is defined as a conceptualization and representation of vulnerability as a causal chain, emphasizing that vulnerabilities are not discrete events.

Vignette

Figure 2 shows a very simple example of a vulnerability chain, where an external trigger disrupts effectiveness of engineering activities, as triggered by increased cost of the commercial software used by the enterprise. This is illustrative of how a rather simple external change may cascade into interim impacts, and ultimately lead to a failure later in the program.

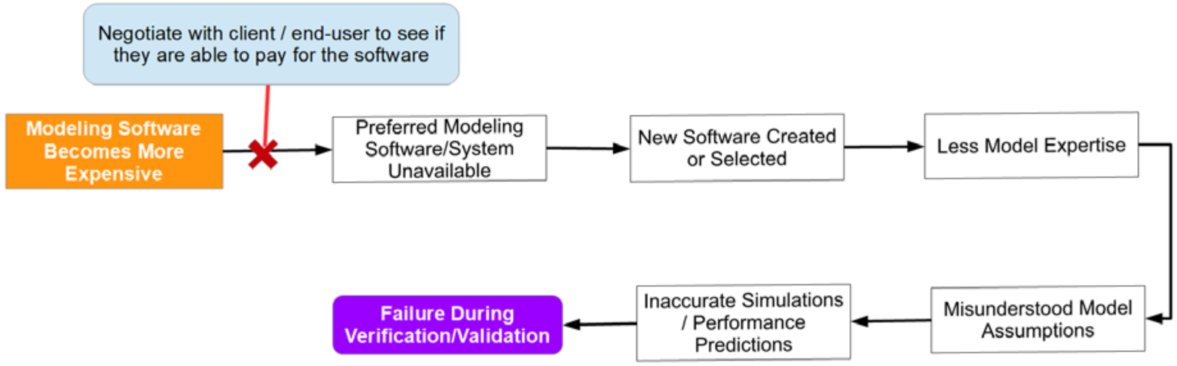

Negotiate with client / end-user to see if they are able to pay for the software
Modeling Software Becomes More Expensive
Preferred Modeling Software/System Unavailable
New Software Created or Selected
Less Model Expertise
Misunderstood Model Assumptions
Inaccurate Simulations / Performance Predictions
Failure During Verification/Validation

Figure 2. **Example Vulnerability Chain With Intervention Point (in Blue)**

Describing this as a vignette, the vulnerability is as follows:

> A particular piece of simulation software that your company has used on similar projects in the past is licensed from commercial software vendor. The license contract is up for renewal soon and the price goes up significantly. This could result in the preferred modeling software being unavailable for use in this program leading to the selection of an alternate software tool that the team has less (or no) experience with. Due to this lack of experience with the new software, assumptions underlying the model may be misunderstood by analysts and thus inaccurate simulation results are generated. This may not be noticed until either verification or validation when the system or subsystem does not behave according to the predicted performance levels.

One identified intervention point is shown in the blue box in Figure 2. Executing this intervention would require that program leadership recognizes when the external trigger is imminent or occurring and act quickly to avoid loss of modeling capability. Alternately, there may be other points of intervention along the chain. While this analysis is quite simple, more sophisticated applications of graph theory and probabilistic modeling can be conducted using a well-developed Reference CEM. For instance, if probabilities, likelihoods, or time scales of each event transition are known, techniques such as Markov Chain Modeling, Monte Carlo Analysis, and Bayesian Networks can be brought to bear, weighting each arc of the graph instead of treating them equally (Reid, 2018).

Cause-Effect Mapping

Cause-Effect Mapping (CEM) has been demonstrated as a useful approach to vulnerability analysis for systems, programs and enterprises (Mekdeci et al., 2012; Rovito & Rhodes, 2016; Reid & Rhodes, 2018a, 2018b). An example CEM for a supply chain case vulnerability assessment (Rovito & Rhodes, 2016) is shown in Figure 3. The hazards are external to the perspective of the defined user, and are thus sometimes called external triggers. An intermediary event is any unintended state change of a system's form or operations which could jeopardize value delivery of the program and/or enterprise. Interventions are actions that eliminate or mitigate a vulnerability to break the causal chain.

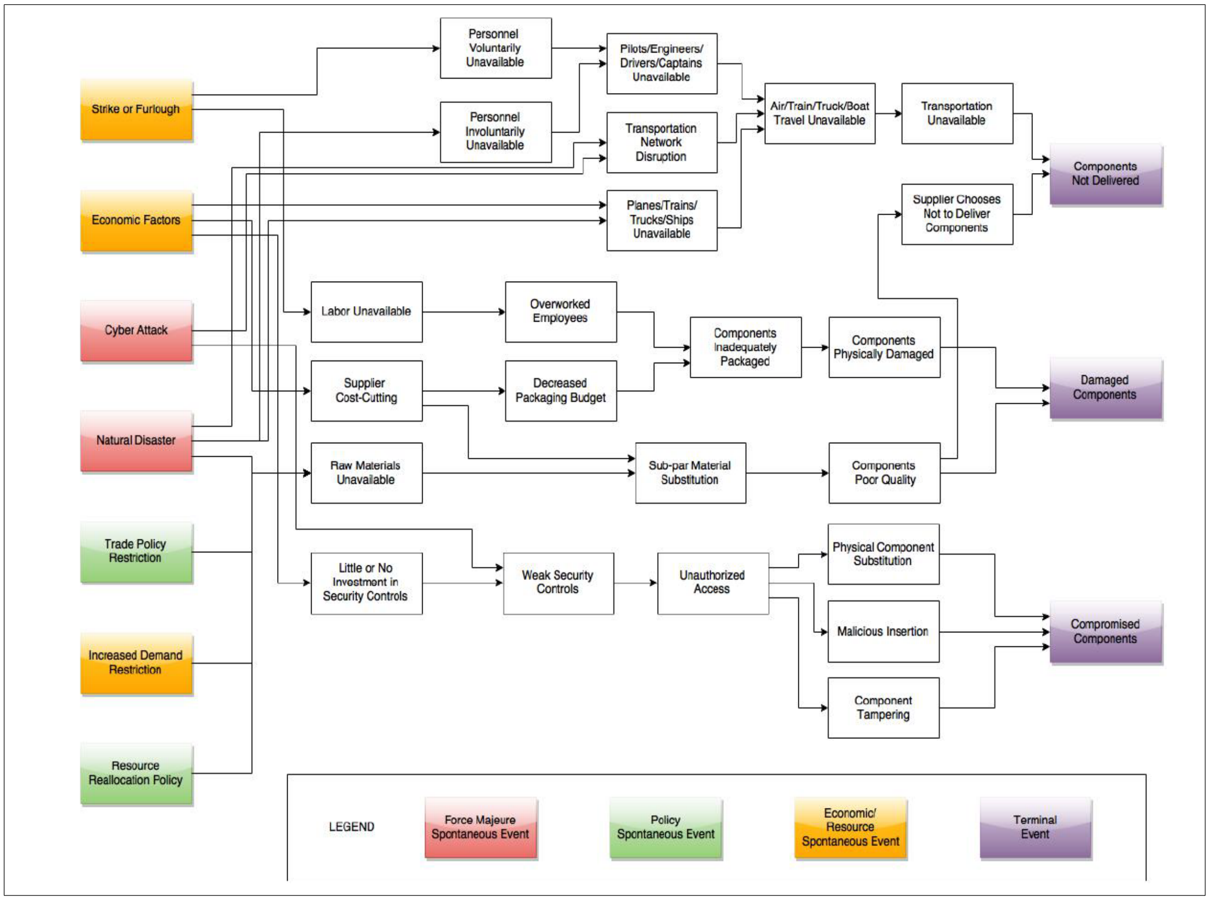
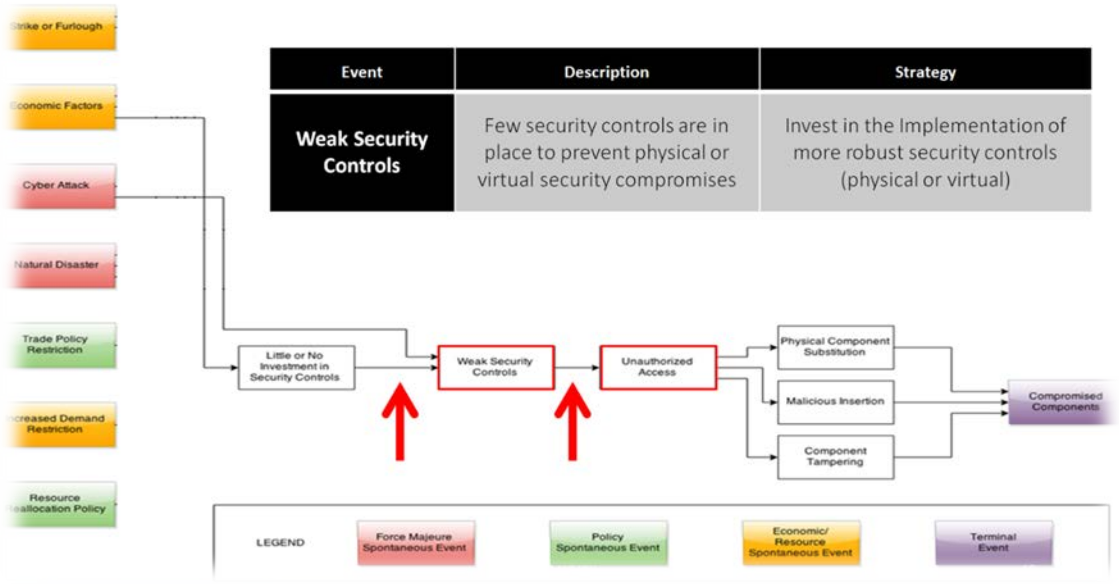

Strike or Furlough
Economic Factors
Cyber Attack
Natural Disaster
Trade Policy Restriction
Increased Demand Restriction
Resource Reallocation Policy
Personnel Voluntarily Unavailable
Personnel Involuntarily Unavailable
Pilots/Engineers/ Drivers/Captains Unavailable
Transportation Network Disruption
Planes/Trains/ Trucks/Ships Unavailable
Air/Train/Truck/Boat Travel Unavailable
Transportation Unavailable
Supplier Chooses Not to Deliver Components
Components Not Delivered
Labor Unavailable
Overworked Employees
Supplier Cost-Cutting
Decreased Packaging Budget
Components Inadequately Packaged
Components Physically Damaged
Damaged Components
Raw Materials Unavailable
Sub-par Material Substitution
Components Poor Quality
Little or No Investment in Security Controls
Weak Security Controls
Unauthorized Access
Physical Component Substitution
Malicious Insertion
Component Tampering
Compromised Components
LEGEND
Force Majeure Spontaneous Event
Policy Spontaneous Event
Economic/ Resource Spontaneous Event
Terminal Event

Figure 3. **Example CEM of a Supply Chain**
(Rovito & Rhodes, 2016)

A CEM is created for a specific class of decision-maker (e.g., program manager). The hazards (referred to as “spontaneous events”) are exogenous from the point of view of the decision-maker for which the CEM was constructed. In this way, the cause-effect mapping approach avoids “blaming someone else” by making all hazards exogenous. The decision-maker has control over only the intermediary events. While not necessarily at fault for any of the vulnerabilities, the decision maker has the responsibility and authority to choose if, and how, to address these.

As shown in Figure 4, a causal chain may have multiple points for breaking the chain, for instance to correct weak security controls and/or to prevent unauthorized access. The first might be a policy/process intervention and the latter might be a technology intervention. The decision to execute one/both of the interventions will depend upon unique factors, such as the cost to implement, color of money available, specifics of the situation, and so forth.



Event	Description	Strategy
Weak Security Controls	Few security controls are in place to prevent physical or virtual security compromises	Invest in the Implementation of more robust security controls (physical or virtual)

Figure 4. **Example of Two Alternative Placements for an Intervention in Causal Chain**

The basic steps to create a new CEM are not application specific and are detailed in Rovito and Rhodes (2016) and Reid and Rhodes (2018b). The stakeholder generates the CEM (or tailors a Reference CEM) by listing potential hazards posed to the program and then traces the consequences of each of these hazards through the intermediary events to the final terminal events. The process is then done in reverse: taking the terminal events, adding in any that are still missing, and working backwards on how these might come about. The causal connections between each intermediary event are examined to see if there are any additional connections not previously noticed. Finally, lessons learned databases, case studies, and other experts are consulted to generate additional hazards, intermediary events, causal connections, and interventions, as well as to verify existing ones. It is envisioned that any of these steps can take place either formally, using automated tools to enumerate possible vulnerabilities, or informally, relying upon the stakeholder's own experience. CEM is fundamentally a qualitative analysis method, though it can be readily adapted into a more quantitative form, by specifying probabilities of transition to each intermediary (Reid & Rhodes, 2018b).

CEM has previously been applied in a case study of a Maritime Security System of Systems (Mekdeci et al., 2012) and to a supply chain case (Rovito & Rhodes, 2016). More recently, an earlier phase of this research developed a Reference CEM for use by program managers to assess enterprise-level vulnerabilities in the digital engineering/model-centric environment (Reid & Rhodes, 2018b). This work, which was based upon literature reviews, interviews with experts, and other sources, sought to provide program leaders with an entry point into for considering such vulnerabilities. Potential use cases are discussed in Reid and Rhodes (2018b). Key benefits include increased understanding of the causal path and the interrelationships between vulnerabilities.

Cause-Effect Map for Model-Centric Programs and Enterprises

CEM provides an effective way to describe cascading vulnerabilities within a digital engineering enterprise. Figure 5 shows the Reference CEM generated in this research using literature reviews and interviews with experts, among other sources. Nineteen intervention points are identified as potential opportunities for breaking causal chains that may be triggered by external events.

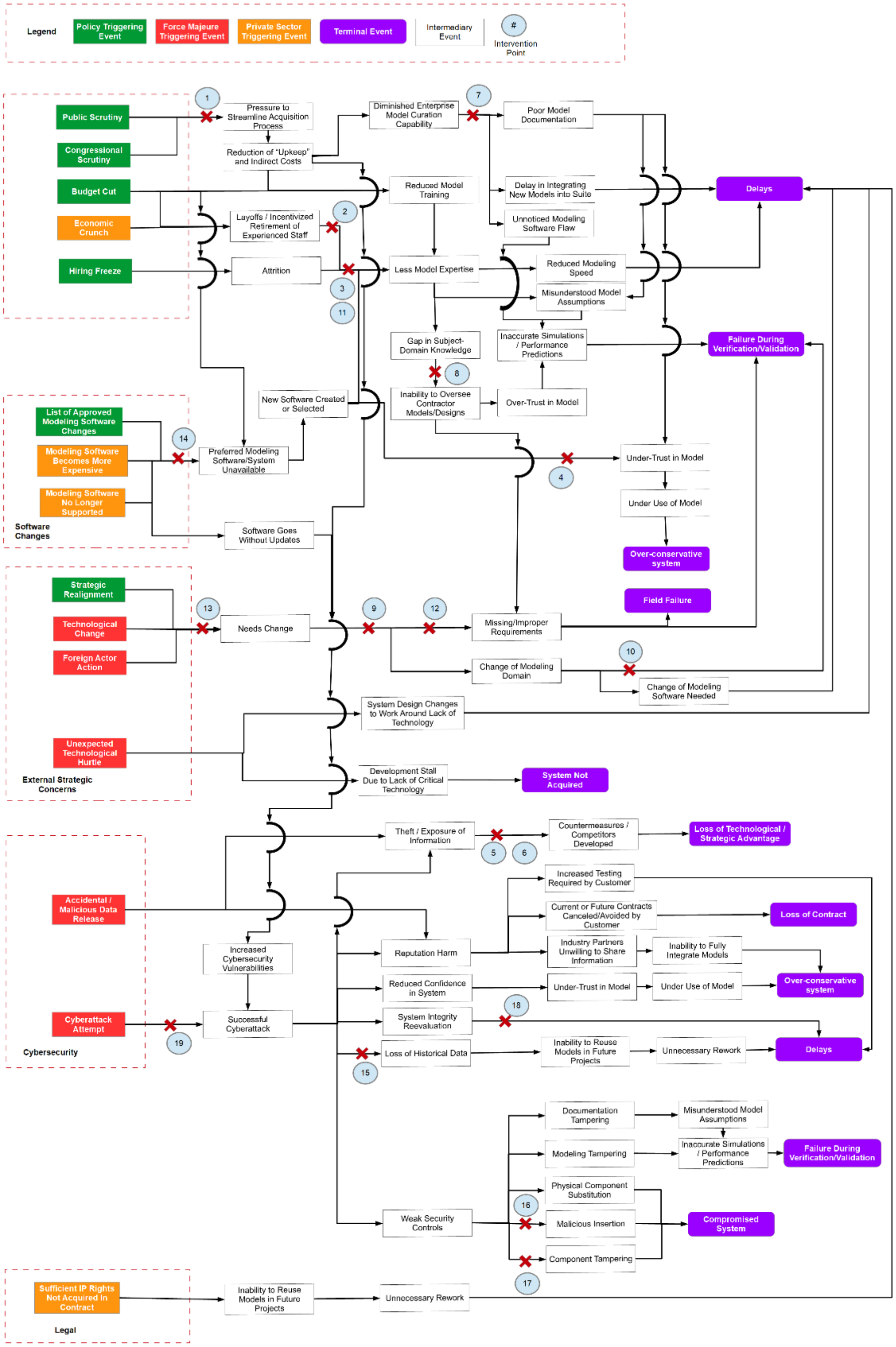

Legend
Policy Triggering Event
Force Majeure Triggering Event
Private Sector Triggering Event
Terminal Event
Intermediary Event
#
Intervention Point
Public Scrutiny
Congressional Scrutiny
Budget Cut
Economic Crunch
Hiring Freeze
1
Pressure to Streamline Acquisition Process
Reduction of "Upkeep" and Indirect Costs
Layoffs / Incentivized Retirement of Experienced Staff
2
Attrition
3
11
Diminished Enterprise Model Curation Capability
7
Poor Model Documentation
Reduced Model Training
Delay in Integrating New Models into Suite
Unnoticed Modeling Software Flaw
Less Model Expertise
Reduced Modeling Speed
Misunderstood Model Assumptions
Delays
Gap in Subject-Domain Knowledge
Inaccurate Simulations / Performance Predictions
Failure During Verification/Validation
8
Inability to Oversee Contractor Models/Designs
Over-Trust in Model
New Software Created or Selected
List of Approved Modeling Software Changes
Modeling Software Becomes More Expensive
Modeling Software No Longer Supported
Software Changes
14
Preferred Modeling Software/System Unavailable
Software Goes Without Updates
Under-Trust in Model
4
Under Use of Model
Over-conservative system
Field Failure
Strategic Realignment
Technological Change
Foreign Actor Action
13
Needs Change
9
12
Missing/Improper Requirements
Change of Modeling Domain
10
Change of Modeling Software Needed
System Design Changes to Work Around Lack of Technology
Unexpected Technological Hurtle
External Strategic Concerns
Development Stall Due to Lack of Critical Technology
System Not Acquired
Theft / Exposure of Information
5
6
Countermeasures / Competitors Developed
Loss of Technological / Strategic Advantage
Increased Testing Required by Customer
Current or Future Contracts Canceled/Avoided by Customer
Loss of Contract
Accidental / Malicious Data Release
Increased Cybersecurity Vulnerabilities
Reputation Harm
Industry Partners Unwilling to Share Information
Inability to Fully Integrate Models
Reduced Confidence in System
Under-Trust in Model
Under Use of Model
Over-conservative system
Cyberattack Attempt
19
Successful Cyberattack
System Integrity Reevaluation
18
Delays
Loss of Historical Data
15
Inability to Reuse Models in Future Projects
Unnecessary Rework
Cybersecurity
Documentation Tampering
Misunderstood Model Assumptions
Modeling Tampering
Inaccurate Simulations / Performance Predictions
Failure During Verification/Validation
Physical Component Substitution
16
Weak Security Controls
Malicious Insertion
Compromised System
Component Tampering
17
Sufficient IP Rights Not Acquired in Contract
Legal
Inability to Reuse Models in Future Projects
Unnecessary Rework

Figure 5. **Reference Cause-Effect Map**
(Reid, 2018)

External triggers that result in similar vulnerability chains are grouped together in the map. By “similar,” we mean that these vulnerability chains either involve many of the same intermediary events or that they involve the same part of the program. For this map, the external triggers were classified into three different domains, defined as follows:

- Force Majeure (red boxes): This is a general term for an event that is the result of actions beyond the possibility of the program enterprise (not just the program manager) to influence. Thus it includes both malicious action and general, unforeseeable events such as Technological Change.
- Policy (green boxes): An event that is the result of intentional decisions made at the organizational or enterprise level. In the case of a government-run program, this includes oversight from Congress and the general public. Non-government organizations may still be impacted indirectly by such oversight, but their proximal triggering event would be different.
- Private Sector (orange boxes): Any event that is the result of the actions of one or more private-sector firms outside the program enterprise.

The purple boxes are the terminal events.

The intervention points on the Reference CEM (Figure 5) are shown in Table 1, where an invention action is defined for each point.

Table 1. Intervention Points for the Reference CEM Shown in Figure 5

(Reid, 2018)

Point #	**Intervention Action**
1	Initiate internal assessment and a public relations strategy
2	Initiate various non-monetary benefits (e.g., 9/80 schedule) to encourage employees to stay
3	Seek to share resources and employees with other programs
4	Hire employees with prior experience with the new software
5	Compartmentalize sensitive information
6	Obfuscate sensitive data with false or misleading information
7	Create documentation and curation processes within the program
8	Institute handover periods to benefit from contractor expertise
9	Reevaluate the training regime and needed fields of expertise
10	Increase the amount of testing conducted
11	Increase use of contractors/consultants to maintain expertise level
12	Reevaluate the requirements with the client and other stakeholders
13	Design for modularity to minimize impact on system
14	Negotiate with client/end-user to see if they are able to pay for the software
15	Maintain isolated but readily accessible back-ups of data
16	Conduct reviews/comparisons of models between lifecycle stages
17	Use multiple independent simulations or component checkers
18	Maintain isolated, independent backup equipment while primary equipment is evaluated
19	Conduct regular “red-team”/penetration test exercises

Observations on Intervention Points

Reid (2018) found that intervention points identified in the Reference CEM (Figure 5) tend to be in the first half of the vulnerability chains, with several immediately after an external trigger. This suggests the need for monitoring for potential or imminent external triggers and being ready to respond as soon as, or even in advance of, their manifestation.

The Reference CEM can be used to guide the attention to various vulnerabilities. For instance, it should be noted that within the “active modeling” set of intermediate events (inside the blue box of Figure 6) there are relatively few intervention points identified, despite the high number of vulnerability chains that pass through that section of the Reference CEM. The primary intervention point identified in that section, number 7, is “Create documentation and curation processes within the program” (see Table 1).

This relative lack of intervention points may represent the unfamiliarity of program leaders with digital engineering processes and how to intervene in them. This suggests that further work would be useful in identifying potential interventions in this section of the map and educating program leaders concerning their availability and use.

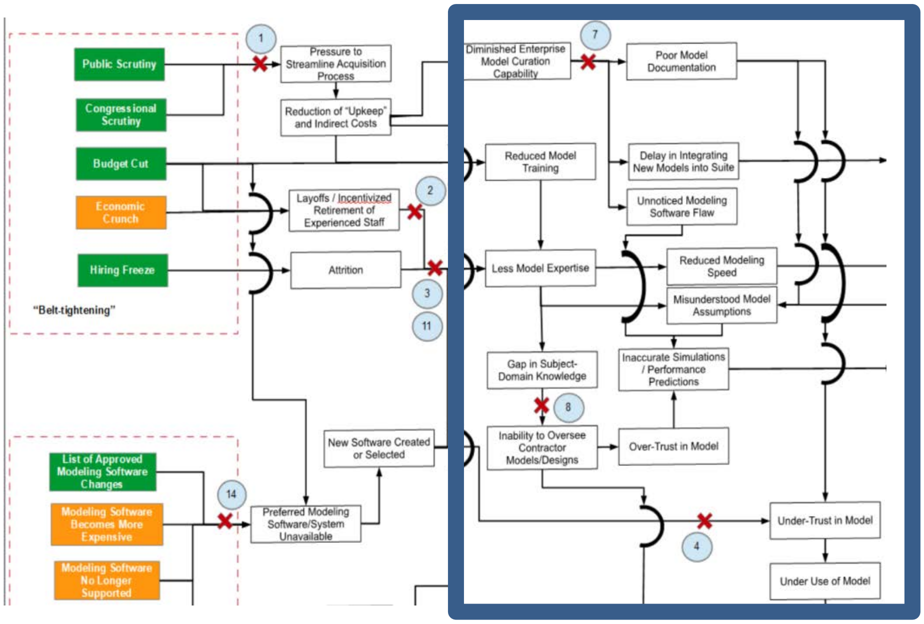

1
Public Scrutiny
Congressional Scrutiny
Budget Cut
Economic Crunch
Hiring Freeze
"Belt-tightening"
Pressure to Streamline Acquisition Process
Reduction of "Upkeep" and Indirect Costs
Layoffs / Incentivized Retirement of Experienced Staff
2
Attrition
3
11
List of Approved Modeling Software Changes
Modeling Software Becomes More Expensive
Modeling Software No Longer Supported
14
Preferred Modeling Software/System Unavailable
New Software Created or Selected
7
Diminished Enterprise Model Curation Capability
Poor Model Documentation
Reduced Model Training
Delay in Integrating New Models into Suite
Unnoticed Modeling Software Flaw
Less Model Expertise
Reduced Modeling Speed
Misunderstood Model Assumptions
Gap in Subject-Domain Knowledge
Inaccurate Simulations / Performance Predictions
8
Inability to Oversee Contractor Models/Designs
Over-Trust in Model
4
Under-Trust in Model
Under Use of Model

Figure 6. **Excerpt of the Reference CEM Highlighting the “Active Modeling” Portion**

(Reid, 2018)

While this portion of the chain has one intervention identified, certain vulnerability chains have multiple intervention points identified at multiple stages. For instance, several of the vulnerability chains that pass through the Needs Change event have three intervention points each (and the others have at least two), as shown in Figure 5.

According to Reid (2018), this suggests there may not be as much of a concern about these vulnerabilities, due to the multiple options of intervention available and the fact that several are positioned multiple events into the chain, giving significant time for response.

An experienced program leader will find some of the listed intervention points to be common sense. For instance, one of the interventions (number 12) following the Needs Change event (see Table 1) is “Reevaluate requirements with the client and other stakeholders.” This degree of occasional obviousness is not unique to CEM but is true of all vulnerability assessment techniques. The point of these techniques is not just to identify new vulnerabilities and interventions, but to consistently track and assess them so that all options are available. A case in point is that even experienced pilots still use a checklist (and surgeons really should be; Haynes, Berry, and Gawande, 2015).

It should be noted that the Reference CEM shown in this paper does omit vulnerabilities and interventions that are entirely unchanged. For example, practices like the security clearance system and restricting the use of digital storage media will remain necessary, effective interventions that are not significantly impacted by MCE environments. Some historically successful methods may be conflict with MCE environments, for example, the use of SCIFs has been quite successful in preventing unauthorized access to data. The typical use of a SCIF in design, where a small number of engineers work on a task isolated from the outside world, is not directly compatible with an MCE environment structured around model integration and collaboration across teams and locations. While this problem has been previously considered and ways to mitigate this conflict have been proposed (e.g., Reid & Rhodes, 2016), no silver bullet to resolving these tensions exists and it is likely that the increased use of MCE will result in both the exacerbation of some current vulnerabilities and the creation of new ones.

Cybersecurity Vulnerabilities

Literature review and interview-based research have provided useful insights throughout the research. As the initial research progressed, the importance and urgency of considering the cybersecurity vulnerabilities shaped the second phase of study to focus more specifically on these. Reid (2018) conducted interviews with systems engineers and program managers from a variety of fields, including defense, aerospace, manufacturing, and semiconductors. The interviews explored these program cybersecurity vulnerabilities in general, and in context of model-centric approaches. Four issues commonly were cited:

- Cybersecurity needs to be thoroughly considered much earlier than it commonly is, preferably in the proposal generation stage.
- Program managers and systems engineers are sometimes intimidated by cybersecurity issues and thus seek to pass them onto specialists later in the acquisition process.
- MBSE and MCE toolset developers and proponents have not done a thorough enough job of considering programmatic cybersecurity vulnerabilities, though the tools are thought to be quite effective at designing for cybersecurity in regard to end-systems.
- Traditional programmatic cybersecurity defensive practices tends to quite effective in traditional engineering programs, but the increased use of MCE, particularly for multi-site collaboration, could change this (Reid & Rhodes, 2018a).

Non-Technical Influences and Impacts

One set of vulnerabilities that came up repeatedly in both the interviews and experiment sessions in our research (Reid & Rhodes, 2018a) were those that passed through the reputation harm intermediate event, as shown in Figure 7.

Despite the frequency that the potential for this vulnerability was raised by experts, few interventions were proposed for post-breach. According to Reid (2018), this suggests that leaders of digital engineering enterprises may need better understanding of potential vulnerabilities leading to breaches in context of digital engineering, as well as more knowledge on how to respond to breaches, particularly prominent ones, instead of solely how to prevent them. While there is evidence in the private sector suggesting that the reputation harm incurred by a prominent breach does not significantly impact the firm (Lange & Burger, 2017), contractors to the government are known to suffer significant financial penalties due to breaches, even when such a breach is unrelated to their government duties (Braun, 2014; Overly, 2017). In a defense acquisition environment, there is thus significant incentive to having program leadership (and the enterprise as a whole) well-prepared to respond to major breaches.

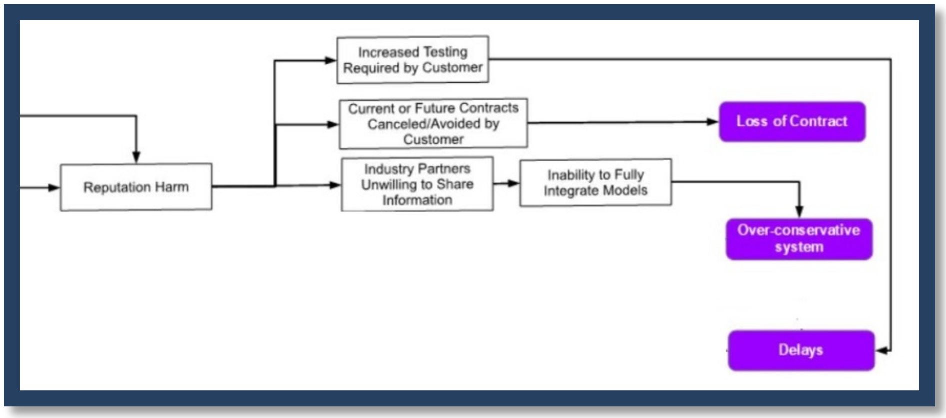

Increased Testing Required by Customer
Current or Future Contracts Canceled/Avoided by Customer
Loss of Contract
Reputation Harm
Industry Partners Unwilling to Share Information
Inability to Fully Integrate Models
Over-conservative system
Delays

Figure 7. **Reputation Harm Vulnerabilities**
(Reid, 2018)

Relevant Research From Other Fields

Huff, Medal, and Griendling (2018) present a methodology for performing vulnerability assessment and decision analysis of critical infrastructure using the approach of model-based systems engineering. The work focuses on physical security of critical infrastructure. Some of their findings may provide useful insights for vulnerability assessment of infrastructure within model-centric enterprises.

The literature on the manufacturing sector offers interesting observations and new research of relevance to vulnerability assessment of model-centric enterprise environments. Burnson (2017), discussing a recent Deloitte study on cyber vulnerabilities in manufacturing supply chains, states “one-third of all manufacturers sampled admitted to not having performed any cyber risk assessments of the industrial connected devices operating on factory floors.” While data is not available, from discussions with experts in the engineering domain, it seems likely that there would be a similar situation in regard to whether cyber risk assessments have been performed for model-centric engineering environments with connected hardware and software.

DeSmit et al. (2016) discuss research on cyber-physical vulnerability assessment in manufacturing systems that uses an approach that employs intersection mapping. According to these authors, “no literature is aimed at assessing cyber-physical vulnerabilities for manufacturing systems.” With similarities of manufacturing facilities with facilities used in model-centric enterprises, their research may offer useful insights to our research. DeSmit et al. (2016) describe their approach as “based on the principle that vulnerabilities in manufacturing systems occur at intersections (and intra-sections, referred to collectively as intersections) of cyber, physical, cyber-physica,l and human entities that embody a manufacturing system.” Similar to the CEM approach, their method maps intersections and assesses the impact at intersection nodes. They evaluate five characteristics: loss of information, inconsistency, relative frequency, lack of maturity, and time until detection. In their method, vulnerability impact assessment (Low, Medium High) is assessed for the characteristics at each of the nodes. This offers an interesting approach to qualitative assessment measures for vulnerability. Another noteworthy facet of their work that resonates with our research is that human entities are included in defining intersections.

Discussion

Knowledge gathered in this research indicates that program leaders do not formally grapple with vulnerabilities within the program and overall enterprise to the extent they do with vulnerabilities related to the end-system. Cause-Effect Mapping, with re-conceptualizing vulnerabilities as causal chains, enables program and enterprise leaders to identify connections, categories, and potential interventions in the vulnerability chains. The research indicates identifying external triggers and representing vulnerabilities as chains enables a more detailed assessment of how interim cascading events can result in significant terminal outcomes. Use of the CEM approach assists in understanding these causal chains, and decomposes a vulnerability in a manner that encourages finding multiple options for mitigation. Particular choices for disrupting a harmful causal chain are useful for considering where and when to place interventions based on the specific nature of the situation.

Limitations

While a fully-developed generalized CEM Reference Map could provide overall benefit to digital engineering programs, the fact that enterprise and programs are unique makes it difficult to accomplish this without much more extensive application and study. Secondly, digital engineering practice and supporting infrastructure are still evolving, so limited knowledge exists at present. Nonetheless, programs and enterprises may derive significant benefit by the activity of constructing a reference map for their unique situation. The process of generating the map invokes thoughtful discussion and anticipating potential hazards that may have been introduced as a result of the digital transformation. The approach of considering vulnerabilities as casual chains yields rich discussion, regardless of whether an overall map is developed. This research has demonstrated the approach to constructing a CEM Reference Map and illustrates content included in the map; a fully-developed comprehensive reference map will require a more extensive investigation.

Research Directions

There are several areas of desired future research direction. First, additional study is needed on leading indicators of vulnerability in digital engineering enterprises, along with potential mitigation strategies. Specific approaches to quantification of interventions in breaking vulnerability causal chains is desired, as related to cost, benefit, importance, frequency, etc. Additional research on dynamic simulation using System Dynamics (SD) with CEM is a promising area to explore given the complexities that will be inherent in a fully populated reference CEM (further discussion is found in Reid, 2018). Implementation of an interactive method used to perform vulnerability assessment using a reference map is a future area of inquiry. Additional research is needed to identify relevant investigation in the systems engineering field; for example, Wach and Salado (2018) describe a plan to discover patterns of unknown vulnerabilities associated with SysML. And, further collaborative research with government and industry is desired to identify additional vulnerability chains and enable testing and scaling the method.

Summary

In summary, digital engineering transformation naturally introduces new vulnerabilities within programs and enterprises. Causal chains provide a useful way to understand how external triggers lead to cascading intermediate events that result in specific outcomes. Understanding a vulnerability chain provides program leaders with increased knowledge and options for inserting interventions to avoid undesired vulnerability outcomes. With more experience and knowledge of vulnerabilities inherent in digital engineering practice and infrastructure, the systems community may find it valuable to establish a generalized Reference CEM that can guide future programs and enterprises to assess and manage vulnerabilities, leading to more successful program outcomes. Related research on model curation views a CEM Reference Map as an enabling tool (Rhodes, 2019) for vulnerability assessment of enterprises.

References

Braun, S. (2014, September 10). OPM plans to terminate contracts with USIS. Federal News Radio. Retrieved from https://federalnewsradio.com/management/2014/09/opm-plans-to-terminate-contracts-with-usis

Burnson, P. (2017, March). New Deloitte study identifies cyber vulnerabilities in manufacturing supply chains. Supply Chain Management Review. Retrieved from https://www.scmr.com/article/new_deloitte_study_identifies_cyber_vulnerabilities_in_manufacturing_supply

DeSmit, Z., Elhabashy, A., Wells, L., & Camelio, J. (2016). Cyber-physical vulnerability assessment in manufacturing systems. In 44th Proceedings of the North American Manufacturing Research Institution of SME (Procedia Manufacturing), 5, 1060–1074.

DoD. (2018, June). Department of Defense systems engineering strategy. Retrieved from https://www.acq.osd.mil/se/docs/2018-DES.pdf

German, E. S,. & Rhodes, D. H. (2017, May). Model-centric decision-making: Exploring decision-maker trust and perception of models. In Proceedings of the 15th Conference on Systems Engineering Research.

Haynes, A. B., Berry, W. R., & Gawande, A. A. (2015, May). What do we know about the safe surgery checklist now? Annals of Surgery, 261(5), 829–830.

Huff, J., Medal, H., & Griendling, K. (2019, March). A model-based systems engineering approach to critical infrstructure vulnerability assessment and decision analysis. Systems Engineering. 22, 114–133.

Lange, R., & Burger, E. W. (2017). Long-term market implications of data breaches, not. Journal of Information Privacy and Security, 13(4).

LeSaint, J., Reed, M., & Popick, P. (2015, April). System security engineering vulnerability assessments for mission-critical systems and functions. In 2015 Annual IEEE Systems Conference (SysCon) Proceedings (pp. 608–613).

Mekdeci, B., Ross, A. M., Rhodes, D. H., & Hastings, D. E. (2012, March). A taxonomy of perturbations: Determining the ways that systems lose value. In Proceedings of the 6th Annual IEEE Systems Conference. IEEE.

Overly, S. (2017, October). IRS temporarily suspends contract with Equifax. Politico. Retrieved from https://www.politico.com/story/2017/10/12/irs-equifax-contract-suspended-243732

Reid, J. B. (2018). Assessing and mitigating vulnerability chains in model-centric acquisition programs (Master's thesis). Cambridge, MA: Massachussetts Institute of Technology.

Reid, J. B., & Rhodes, D. H. (2016, March). Digital system models: An investigation of the non-technical challenges and research needs. In Proceedings of the Conference on Systems Engineering Research.

Reid, J. B., & Rhodes, D. H. (2018a, May). Applying cause-effect mapping to assess cybersecurity vulnerabilities in model-centric acquisition program environments. In Proceedings of the 15th Annual Acquisition Research Symposium. Monterey, CA: Naval Postgraduate School.

Reid, J. B., & Rhodes, D. H. (2018b, May). Assessing vulnerabilities in model-centric acquisition programs using cause-effect mapping. In Proceedings of the 15th Annual Acquisition Research Symposium. Monterey, CA: Naval Postgraduate School.

Reymondet, L., Rhodes, D. H., & Ross, A. M. (2016, April). Considerations for model curation in model-centric systems engineering. In Proceedings of the 10th Annual IEEE Systems Conference. IEEE.

Rhodes, D. H. (2018, April). Using human-model interaction heuristics to enable model-centric enterprise transformation. In Proceedings of the 12th Annual IEEE Systems Conference. IEEE.

Rhodes, D. H. (2019, April). Model curation: Requisite leadership and practice in digital engineering enterprises. In Proceedings of the 17th Conference on Systems Engineering Research.

Rovito, S. M., & Rhodes, D. H. (2016, April). Enabling better supply chain decisions through a generic model utilizing cause-effect mapping. In Proceedings of the 10th Annual IEEE Sytems Conference. IEEE.

Wach, P., & Salado, A. (2018, March). A research plan to discover patterns of unknown vulnerabilities associated with adopting SysML. In Proceedings of the 16th Conference on Systems Engineering Research.

Acknowledgement & Disclaimer

This material is based upon work supported by the Acquisition Research Program under Grant No. HQ00341810013. The views expressed in written materials or publications, and/or made by speakers, moderators, and presenters, do not necessarily reflect the official policies of the Department of Defense nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Risk Management and Information Assurance Decision Support

Hanan Hibshi—is a Research and Teaching Scientist at the Information Networking Institute at Carnegie Mellon University. Dr. Hibshi's research area includes: usable security, security requirements, and expert's decision-making. Dr. Hibshi's research involves using grounded theory and mixed-methods user experiments to extract rules for use in intelligent systems. Dr. Hibshi received a PhD in Societal Computing from Carnegie Mellon University, an MS in Information Security Technology and Management from the Information Networking Institute at Carnegie Mellon University, and a BS in Computer Science from King Abdul-Aziz University in Jeddah, Saudi Arabia. [hhibshi@cmu.edu]

Travis D. Breaux—is an Associate Professor of Computer Science, appointed in the Institute for Software Research of the School of Computer Science at Carnegie Mellon University. Dr. Breaux's research program searches for new methods and tools for developing correct software specifications and ensuring that software systems conform to those specifications in a transparent, reliable and trustworthy manner. This includes demonstrating compliance with U.S. and international accessibility, privacy and security laws, policies and standards. Dr. Breaux is the Director of the Requirements Engineering Laboratory at Carnegie Mellon University. Dr. Breaux has several publications in ACM- and IEEE-sponsored journals and conference proceedings. Dr. Breaux is a member of the ACM SIGSOFT, IEEE Computer Society, and USACM Public Policy Committee. [breaux@cs.cmu.edu]

Abstract

Like any organization, the DoD still relies on security analysts who can ensure that security requirements are satisfied. Relying on one expert's opinion can be risky, because the degree of uncertainty involved in a single person's decision could increase with time, memory failure, or inexperience. In previous work, we introduced the multifactor quality measurement method (MQM) where we reduce this risk by collecting security ratings from multiple experts with documented expertise in specific technical areas of cybersecurity. The next step is to automate the scenario generation where less experienced IT personnel can create scenarios that correspond to their own system architecture using our tool. The automation allows one to crowdsource security assessments from experts. The tool will collect and analyze the expert ratings and return the results to the original requestor. In this paper, we propose our designed prototype for the tool and we share the results of evaluating the prototype on 30 students who are completing a master's degree in cybersecurity at Carnegie Mellon University. Based on the qualitative and usability analysis of responses, our proposed method is shown effective in systematic scenario elicitation. Participants had a 100% task completion rate with 57% of participants achieving complete task-success, and the remaining 43% of participants achieving partial task-success. Finally, we discuss our findings and future directions for this research in systematic scenario elicitation.

Introduction and Background

Organizations, including the DoD, rely on security experts to evaluate system security and determine appropriate mitigations (Garfinkel, 2005, p. 5; Hibshi, 2016; Hibshi, Breaux, & Broomell, 2015). Despite the abundance of requirements that are available in security checklists and control sets, such as the NIST 800-53 control set ("NIST/ITL Special Publication (800)," 2015) security analysts continue to rely on their own experience and background knowledge when analyzing system security (Hibshi et al., 2015; Hibshi et al., 2016). Checklists are convenient because they generally apply to systems; however, they lack the context needed to assess the threat against a specific configuration (Haley et al., 2008). Claims that negative events are unlikely is difficult without being explicit about one's trust assumptions (Haley et al., 2008). Moreover, mapping the checklist to threat scenarios or other requirements is laborious process repeated by an analyst for each system. Finally, security requirements are not independent; instead, they work together in composition with different priorities and inter-dependencies to improve overall security (Garfinkel, 2005, p. 5).

Recently, we examined the effect of context and requirements composition on security requirements expert ratings (Hibshi et al., 2015; Hibshi & Breaux, 2017). In that work, we used factorial vignettes in which requirements and system constraints are variables in a scenario description. We use scenarios from four technical areas: networking, operating systems, databases, and web applications (Hibshi et al., 2015; Hibshi & Breaux, 2017). The result is a new method that we call the multifactor quality measurement (MQM) method. The MQM process, which relies on using scenarios expressed in natural language text, would greatly benefit from introducing automation. The automation would involve using a tool where less experienced IT personnel can create scenarios that correspond to their own system architecture. The IT personnel could crowdsource security assessments from experts, and the tool would then analyze the collected data and send the results back to the IT personnel.

In this paper, we prototype the tool for scenario elicitation from IT personnel. Since eliciting scenarios in natural language text format can be an ad hoc process with possible ambiguity, we build our tool prototype using a scenario language based on a simplified process model of iterative scenario refinement. The model consists of three steps: (1) eliciting an interaction statement that describes a critical action performed by a user or system process; (2) eliciting one or more descriptive statements about a technology that enables the interaction; and (3) refinement of the technology into technical variants that correspond to design alternatives. In the upcoming sections of this paper, we will provide more details about the prototyped model and the results of its evaluation.

Systematic Scenario Elicitation

We now describe our approach to study the activity of systematic scenario elicitation. The approach assumes a model of structured scenario elicitation that results in a user story (Cohn, 2004) in natural language text that we refer to as scenario throughout this paper. To describe the model, consider the example text scenario shown in Figure 1. The example starts with an *interaction statement*, which is a statement that describes a critical action performed by a user or a system process. The *interaction statement* used in the example is specific to a domain (healthcare) but can also be stated more generically with no domain. Next, appears the *descriptive statement*, which describes a technology that enables the interaction.

For any type of technology, based on the stakeholder's needs and environment, there could be a variety of design alternatives to identify. To accommodate this diversity, the model allows a stakeholder to define a *variable* for a technology and list the design alternatives as different *levels* of that variable. In the example shown in Figure 1, we define a $Network variable with three possible levels.

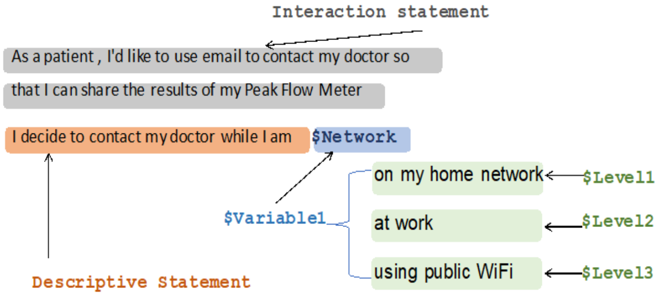

Interaction statement
As a patient , I'd like to use email to contact my doctor so
that I can share the results of my Peak Flow Meter
I decide to contact my doctor while I am
$Network
on my home network
$Level1
at work
$Level2
using public WiFi
$Level3
$Variable1
Descriptive Statement

Figure 1. **Example of a Text Scenario**

The model is intentionally limited to these three elements: *interaction statement*, and one or more *descriptive statements* that each contains a variable with *levels*. This limitation is necessary to identify and isolate sources of error in scenario generation. In the future, one could imagine studying more advanced scenarios with nested levels of interaction and description.

Stakeholder Input

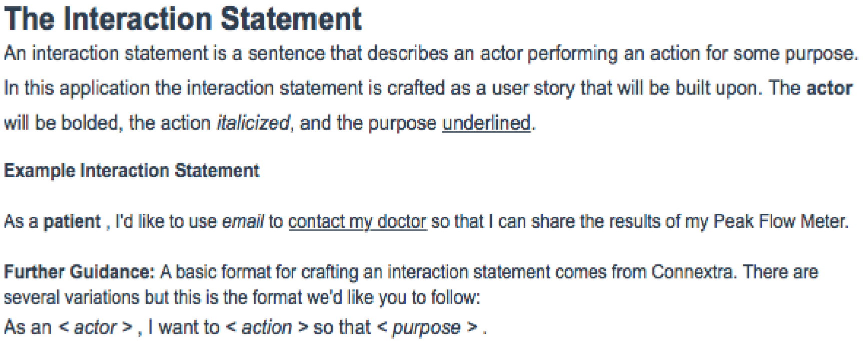
To elicit scenarios from stakeholders, our approach involves three steps corresponding to the model elements described above:

1. *Interaction statement elicitation*: where stakeholders are asked to provide a domain of interest and a related interaction statement in the following format:

   As an **< actor >**, I want to **< action >** so that **< purpose >**.

2. *Descriptive statement(s) elicitation*: where stakeholders are asked to provide one or more descriptive statements.
3. *Technology refinement:* where stakeholders define variables to represent the chosen technology and define a number of levels representing different design alternatives. After defining their own variables, stakeholders are asked to rank these variables based on a certain quality (e.g., security).

Scenario collection from users is completed online through online forms that prototypes the forms used in the design of the tool. The scenario elicitation process is accompanied with explanatory text and training material. For example, we use the text shown in Figure 2 to explain interaction statements to stakeholders. We follow a similar approach to explain the descriptive statements, the variables, and the levels.



The Interaction Statement

An interaction statement is a sentence that describes an actor performing an action for some purpose.

In this application the interaction statement is crafted as a user story that will be built upon. The **actor** will be bolded, the action *italicized*, and the purpose underlined.

Example Interaction Statement

As a **patient** , I'd like to use *email* to contact my doctor so that I can share the results of my Peak Flow Meter.

Further Guidance: A basic format for crafting an interaction statement comes from Connextra. There are several variations but this is the format we'd like you to follow:
As an < *actor* > , I want to < *action* > so that < *purpose* > .

Figure 2. **Training and Example Text for the Interaction Statement of a Text Scenario**

Evaluation of the Model

We designed a prototype and test the model on stakeholders in the form of an online survey. The survey consists of several forms that corresponds to the forms used in the prototype. Our target population is stakeholders interested in the cybersecurity domain. At the beginning of the survey, we explain to participants that the end goal of these tasks is to construct a *vignette,* which we define to participants of the survey as: *a story that people read before making an important decision. The vignette adds context to help the person make a more informed decision*.

Going through each step in the model, we provide stakeholders with definitions and running examples to help understand the concepts needed to perform the task related to that step (see Figures 1 and 2). The study participants are asked to provide their input following each explanation and training. For example, following the training shown in Figure 2, participants are asked to provide an interaction statement for their domain of interest (they have been presented with training materials and example domains prior to being introduced to the interaction statement).

Upon task completion, we ask participants to rate their own experience performing the tasks in the user study. We ask them to rate the difficulty of each individual task on a 7-point scale. In addition, we ask participants about the likelihood (using a 7-point scale) of using a tool for scenario creation that is similar in design to the exercise that they just completed. We repeat this likelihood-of-use question twice: for someone inside the participant's organization, and for someone outside the participant's organization. This repetition encourages participants to think more broadly about the possible broader benefits of the tool prototype that they just have tried even if they do not see a direct benefit to themselves in using such tool. We also allowed participants to provide additional open-ended comments.

Lastly, we ask participants to answer 14 security knowledge questions and standard demographic questions (e.g., gender, age, and years of experience).

We recruited participants from who are enrolled in a well-recognized information security master's degree program in a top university in the United States. Each participant was compensated with a $25 Amazon gift card.

Analysis of Participant Responses

We are interested in the effectiveness, efficiency, and user-satisfaction of the proposed three-step scenario elicitation model. We next describe how we analyze and measure these components:

- **Effectiveness** is concerned with a stakeholder success in completing a task while maintaining an acceptable level of accuracy (**Frøkjær**, Hertzum, & Hornbæk, 2000). In our results we measure effectiveness using task completion rates. To account for task accuracy, we differentiate between *full task success*, where participants complete the task with no missing information or errors; and *partial task success* where participants complete the task with some errors or missing information.

- **Efficiency** is concerned with the resources a stakeholder consumes to complete a task while maintaining an acceptable level of accuracy (**Frøkjær** et al., 2000). In our study, we use *task completion time* to measure efficiency.

- **Satisfaction** is concerned with stakeholders' attitudes when using a system (**Frøkjær** et al., 2000). To measure participants satisfaction with our model, we use rating scales to ask study participants to provide their perception of task difficulty and their projection of likelihood-of-use.

The constructs shown above rely on qualitative analysis of study participants responses. We use grounded analysis (Corbin & Strauss, 2007; Glaser, 1978) and coding theory (Saldaña, 2012) to code participants open-ended, text responses. The following is an explanation of how we analyzed the data to help measure the three constructs listed above and to provide qualitative insights.

- **Domains:** Participants were asked to list their domains of interest and the interaction statement. Using open coding, we review participant answers and categorize the elicited domains into a broader domain category. For example, the forensics domain is categorized into the broader domain of cybersecurity, and the banking domain is categorized into the broader domain of finance (finance can include corporate investment for example).
- **Interaction Statement:** A full interaction statement should contain the actor, action, and purpose. We coded interaction statements as *complete* if the participant provides a full interaction statement, and *incomplete* if participant provided an interaction statement that is missing the purpose. We coded empty responses with N/A, and non-statement responses (e.g., words and phrases) as not provided.
- **Descriptive Statement:** A correct descriptive statement should follow the format shown in the example shown in Figure 1 and must contain a variable preceded by the ($) sign. We coded descriptive statements as *correct* if the participant provides a descriptive statement using a format similar to the training, *partial* if the participant provides partial text that still can be comprehensible as a descriptive statement but is missing the variable or the dollar sign ($) preceding the variable, and *incorrect* if otherwise. We also coded the relationship between descriptive statements and interaction statements with one of the following codes: *related* if a strong relationship can be derived from the text; *semi-related* if the relationship can be derived but is not obvious; and *not related* if otherwise.
- **Variables:** Initially, we coded a variable *correct* if it correctly represents a technology that can have multiple design alternatives (levels), and incorrect otherwise. Later, we added the code: *level* if the variable is not perceived as a broader category of its level, but rather is perceived as another level (e.g., the variable "home network" is coded as level, if the participant provides "employer network" and "public network" as levels). Variables that are missing the dollar sign ($) are coded as *partial*.
- **Variable/level structure:** We coded the structure as *correct* if the participant provided variables and levels in the expected format where variables are a broader technology category of the levels, and we coded the variable/level structure to be *incorrect* if otherwise.

Training material used in the experiment includes an example of a $Network variable with three possible levels (see Figure 1). The levels shown to participants are technical variants of different network configurations that vary in their security strength (some levels are more secure than others). For each variable/level combination, we assigned codes that best describe the relationship between the levels and the variable they are supposed to refine. In cases where the variable is missing or wrong, then we code the relationship between the levels themselves. The codes, or concept labels, follow the Glassier view of *open coding*, wherein the codes emerge from the data without any pre-defined initial code set (Glaser, 1978).

Inter-Rater Reliability

When coding qualitative data that is subject to different interpretations, it is recommended to use multiple raters and calculate inter-rater reliability where researchers use statistical measures like Cohen's Kappa to measure above chance agreement (Cohen, 1968) and be able to judge the quality of the code set being used (Cohen, 1968; Saldaña, 2012). We use two coders for our data set (the first and second authors), and we calculate Cohen's Kappa for each coded data type separately. Our calculated Kappa averaged at 0.9, which is considered good agreement (Cohen, 1968). Next, the disagreements were resolved to reach complete agreement to finalize the dataset for analysis.

Results

We now present our analysis results. We collected scenarios from 30 participants. The mean time that a participant used to complete the scenario elicitation tasks including training is 24 minutes.

Demographics

All participants have a bachelor's degree in computer science or a related field and are currently enrolled in a graduate information security program at a top U.S. university. Out of the 30 students, three participants already work for industry and one works for the U.S. government. The mean score for participants on the security knowledge test is 58%. Table 1 summarizes the demographics statistics of study participants.

Table 1. Demographics Information

Description		**Participants**	
		Number	*Percentage*
Gender	Male	21	70%
	Female	8	27%
	Prefer not to say	1	3%
Years of Computer Security Experience (Mean=2)	Less than 1	6	20%
	1–2 years	13	43 %
	3–4 years	7	23 %
	5–7 years	4	13%
Age range	18–24	18	60%
	25–34	12	40%
Took job training in security		27	40%
Self-taught security knowledge		12	57%
Security Knowledge Score	Scored above 60%	12	31%
	Scored between 40% and 60%	16	41%
	Scored below 40%	2	5%

Task Completion

All 30 participants completed the user study from start to end, and they provided a domain of interest. The task completion rate that maps to our research questions is related to constructing a scenario using the three steps of providing an interaction.

We define three completion categories: full completion when a participant completes the interaction statement and at least one descriptive statement with its associated variables and levels with full accuracy; partial completion if a participant completes the interaction statement and at least one descriptive statement with its associated variables and levels with partial accuracy; and failure if a participant did not provide an interaction statement and did not provide any description statements with an associated variable. Since our evaluation of responses relies on qualitative analysis, we show in Table 2 how we classify full accuracy vs. partial accuracy based on the codes used in the grounded analysis.

Based on our definitions above, our study data shows that 57% of participants achieve full completion (17 responses), 43% achieve partial completion (13 responses), and 0% failures.

When analyzing the 13 partial completions, we found four participants providing incomplete interaction statements that did not include a purpose, five participants did not precede the variables with a dollar sign ($), three participants used another level instead of a broader category for levels, and one participant who provided a variable with levels that do not relate or show a clear variable/level structure.

Table 2. Tasks Accuracy Definitions Based on Codes

Coded Task	Codes		
	Full accuracy	Partial accuracy	Failure
Interaction statement	complete	incomplete	Not provided, N/A
Descriptive statement	correct	partial	incorrect
Variable	correct	partial, level	incorrect

Participant Satisfaction

We measure participants interaction using participants ratings of task difficulty and likelihood of use. All 30 participants provided ratings for task difficulty and likelihood of use, and only eight participants provided additional open-ended comments.

Task Difficulty

Table 3 summarizes the participant feedback about the task difficulty involved in scenario creation. For the first four tasks: understanding vignettes (i.e., scenarios), understanding interaction statements, crafting interaction statements, and understanding descriptive text; almost half (between 48–63%) of participants were skewed toward easy ratings (somewhat easy, easy, and very easy combined). For the later four tasks shown in Table 3, participants feedback is less skewed in any direction. By assigning numeric values to the 7-point scale (with 1=Very Easy and 7= Very Hard), we found that the mean value for all tasks ranges between 3.1 and 3.9, which is slightly below Neutral (Neutral=4), leaning towards the easy category.

Table 3. Participants Feedback About Task Difficulty

Task	ery Easy	asy	omewhat Easy	eutral	omewhat Hard	ard	ery Hard
Understanding vignettes	13%	33%	7%	27%	17%	3%	0%
Understanding interaction statements	7%	27%	30%	20%	10%	3%	3%
Crafting interaction statements	3%	14%	31%	24%	21%	0%	7%
Understanding descriptive text	3%	20%	33%	20%	17%	3%	3%
Crafting descriptive text	0%	13%	30%	13%	40%	3%	0%
Understanding variables	7%	17%	17%	30%	23%	3%	3%
Crafting variables	7%	7%	23%	23%	30%	7%	3%
Understanding levels	10%	13%	13%	27%	17%	10%	10%
Crafting levels	7%	13%	20%	27%	17%	7%	10%

Likelihood-of-Use

Table 4 summarizes participant feedback about the likelihood of using a tool similar to what was presented in the study by the participants themselves or someone else inside or outside their organization. In general, participants were slightly more skewed towards unlikely. Three participants explained in their open-ended comments that they did not fully understand the end goal of the tool presented in the survey. By looking at their performance, these three participants still managed to complete the required tasks. These observations suggest that participants might not been able to project the benefit of using the language proposed in the tool, which affected their projection of likelihood-of-use.

Table 4. Participants' Feedback About Likelihood of Using a Vignette Generation Tool

If this tutorial was integrated into an online tool for crafting vignettes that can be used later for running user study, how likely	Very Unlikely	Unlikely	Somewhat Unlikely	Neutral	Somewhat Likely	Likely	Very Likely
would YOU use such a tool	10%	13%	23%	17%	13%	23%	1%
would someone IN your organization use such a tool	10%	3%	7%	33%	27%	17%	3%
would someone OUTSIDE your organization use such a tool	17%	10%	13%	17%	30%	7%	7%

Discussion, Future Work, and Conclusions

In this paper, we introduced a language for scenario elicitation that is based on a three-step model that elicit structured parts of natural language text from stakeholders. When the natural language text parts are combined, the end result is short scenario template with a variable that can take different values of varying levels of technologies. The varying technologies allow us to compare different technology alternatives that can be further evaluated by other analysts, stakeholders, or domain experts. We present results from our evaluation of a user study where we examine the usability of our introduced method. Our analysis results for this preliminary study suggest a promising future in this area, because we had no empty responses or failures. The task completion is 100% divided between 57% full accuracy, and 43% partial accuracy.

Unlike previous research in requirements engineering where scenarios were produced from formal representations that more closely correspond to models, our method relies on guiding stakeholders to create scenarios presented in natural language text. Using a structured approach in collecting statements has shown a benefit in collecting scenarios that share similar syntax and differ in semantics. This uniformity has a number of benefits, as follows:

- **Scalability and more systemized collection process,** where a requirement engineer can tailor our method based on the domain of interest and use it to collect natural language scenarios from a larger participant pool. Systemizing natural language scenario elicitation offers more scalability and coverage compared to collecting unstructured stakeholder narratives.

- **Homogenous stakeholder scenarios** that result from using a structured approach in our method. Scenarios written in natural language are known to be more user-friendly to the stakeholder, but without proper structure, the process becomes ad-hoc and scenarios will be highly heterogenous with no unifying pattern that can help an analyst parse different scenarios. In our results, all elicited scenarios shared a common structure, even in cases where participants had partial accuracy.
- **Systemized scenario analysis,** which is a result of the homogeneity feature of scenarios collected using our proposed method. Following a uniformed syntax is a feature that facilitates the parsing of natural language text, which allows requirements engineers to analyze and validate scenarios using systemized means and automated tools. In our experiment, we were able to systematically analyze the data and we found the process to be less time consuming than analysis done on unstructured natural language text collected, for example, in user interviews and focus groups.
- **Real capture of stakeholder experiences and domain knowledge** because our method allows stakeholders to write scenarios using natural language text, where they only learn a certain structure to arrange their words. In our experiment results, the security domain knowledge was evident in the elicited scenarios.

Going forward, our future research involves introducing more automation to the tool. We envision that using our tool, an analyst would be able to build their own scenario and then send out invitations for experts to rate the overall security and the individual security requirements, and to provide further requirements that can enhance the ratings. Such a tool would have a great impact on the DoD and other organizations in the public and private sectors, because it would help systemize the evaluation of security components using real experts' input.

References

Cohen, J. (1968). Weighted kappa: Nominal scale agreement provision for scaled disagreement or partial credit. *Psychological Bulletin*, *70*(4), 213.

Cohn, M. (2004). *User stories applied: For agile software development*. Addison-Wesley Professional.

Corbin, J., & Strauss, A. (2007). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Thousand Oaks, CA: Sage.

Frøkjær, E., Hertzum, M., & Hornbæk, K. (2000). Measuring usability: Are effectiveness, efficiency, and satisfaction really correlated? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 345–352. The Hague: The Netherlands: ACM.

Garfinkel, S. (2005). *Design principles and patterns for computer systems that are simultaneously secure and usable.* Cambridge, MA: Massachusetts Institute of Technology. Retrieved from http://dspace.mit.edu/handle/1721.1/33204

Glaser, B. G. (1978). *Theoretical sensitivity: Advances in the methodology of grounded theory*. Mill Valley, CA: Sociology Press.

Haley, C. B., Laney, R., Moffett, J. D., & Nuseibeh, B. (2008). Security requirements engineering: A framework for representation and analysis. *IEEE Transactions on Software Engineering*, *34*(1), 133–153.

Hibshi, H. (2016). Systematic analysis of qualitative data in security. In *Proceedings of the Symposium and Bootcamp on the Science of Security* (p. 52). https://doi.org/10.1145/2898375.2898387

Hibshi, H., Breaux, T., & Broomell, S. B. (2015). Assessment of risk perception in security requirements composition. In *Proceedings of the 2015 IEEE 23rd International Requirements Engineering Conference (RE)* (pp. 146–155).

Hibshi, H., & Breaux, T. D. (2017). Reinforcing security requirements with multifactor quality measurement. In *Proceedings of the 2017 IEEE 25th International Requirements Engineering Conference (RE)* (pp. 144–153). Lisbon, Portugal: IEEE.

Hibshi, H., Breaux, T. D., Riaz, M., & Williams, L. (2016). A grounded analysis of experts' decision-making during security assessments. *Journal of Cybersecurity*. Retrieved from http://cybersecurity.oxfordjournals.org/content/early/2016/10/04/cybsec.tyw010.abstract

Hibshi, H., Breaux, T. D., & Wagner, C. (2016). Improving security requirements adequacy: An interval type 2 fuzzy logic security assessment system. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1–8). Retrieved from http://ieeexplore.ieee.org/abstract/document/7849906/

NIST/ITL Special Publication (800). (2015, January 2). Retrieved from http://www.itl.nist.gov/lab/specpubs/sp800.htm

Potts, C., Takahashi, K., & Anton, A. I. (1994). Inquiry-based requirements analysis. *IEEE Software*, *11*(2), 21–32.

Saldaña, J. (2012). *The coding manual for qualitative researchers*. Thousand Oaks, CA: Sage.

Sutcliffe, A. (1998). Scenario-based requirements analysis. *Requirements Engineering*, *3*(1), 48–65.

U.S. Bureau of Labor Statistics. (2016, March 8). *Information security analysts: Occupational outlook handbook*. Washington, DC: U.S. Bureau of Labor Statistics. Retrieved from http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Van Lamsweerde, A. (2000). Requirements engineering in the year 00: A research perspective. In *Proceedings of the 22nd International Conference on Software Engineering* (pp. 5–19). Retrieved from http://dl.acm.org/citation.cfm?id=337184

Panel 13. Improving Acquisition Results Through Data Analytics

Wednesday, May 8, 2019	
3:45 p.m. – 5:00 p.m.	**Chair: Mark Krzysko,** Director, Acquisition Data, Strategy Data Design, Office of the Under Secretary of Defense (Acquisition and Sustainment) ***Data Enhancement and Analysis of Federal Acquisition Databases*** Ningning Wu, Richard Wang, and Mihail Tudoreanu, University of Arkansas ***Identification and Characterization of Data for Acquisition Category (ACAT) II–IV Programs*** Megan McKernan, Jerry Sollinger, Jeffrey Drezner, Austin Lewis, Ken Munson, Geoffrey McGovern, Devon Hill, Marek Posard, and Jaime Hastings, RAND Corporation ***Evaluating the Use of Public Data Sources to Improve Acquisition Processes: A Market Research Use Case*** Dorcas LaSalle and Kristin Fitzgerald, The MITRE Corporation

Mark Krzysko—insert bio text here

Data Enhancement and Analysis of Federal Acquisition Databases

Ningning Wu—is Professor of Information Science at the University of Arkansas at Little Rock. She received a BS and an MS in Electrical Engineering from the University of Science and Technology of China and PhD in Information Technology from George Mason University. Wu's research interests are data mining, network and information security, and information quality. She holds certificates of the IAIDQ Information Quality Certified Professional (IQCP) and the SANS GIAC Security Essentials Certified Professional. [nxwu@ualr.edu]

M. Eduard Tudoreanu—is Professor of Information Science at University of Arkansas Little Rock. Tudoreanu has expertise in human-computer interaction, information quality, advanced visualization of complex data, and virtual reality. He worked on visual data analysis, and has extensive experience in software development and user interface design. [metudoreanu@ualr.edu]

Richard Wang—is Director of the MIT Chief Data Officer and Information Quality Program. He is also the Executive Director of the Institute for Chief Data Officers (iCDO) and Professor at the University of Arkansas at Little Rock. From 2009 to 2011, Wang served as the Deputy Chief Data Officer and Chief Data Quality Officer of the U.S. Army. He received his PhD in information Technology from the MIT Sloan School of Management in 1985. [rwang@mit.edu]

Wenxue Jiang—is a graduate student in the Information Quality program at University of Arkansas at Little Rock. He has been working on his master project with a focus on quality assessment and integration of acquisition databases. He is expected to graduate with a Master of Science in Information Quality in December 2019. [wxjang@ualr.edu]

Abstract

The Federal Funding Accountability and Transparency Act of 2006 (FFATA) required federal contract, grant, loan, and other financial assistance awards of more than $25,000 be displayed on a publicly accessible and searchable website to give the American public access to information on what the federal government spends every year and how it spends the money. Federal acquisition databases, such as those maintained by usaspending.gov and fpds.gov, serve this purpose. These databases contain contract information for all U.S. departments for the last 20 years. However, little has been done to dig into the data and extract the information that may provide valuable insights on potential ways to improve the efficiency of acquisition management. This paper takes a data science approach to assessing and enhancing the quality of the databases and to discovering patterns that can be potentially useful for acquisition research and practice.

Introduction

Defense acquisition consists of different data silos. These data silos have both technical and cultural origins. The capabilities to draw upon data across information systems hold huge potential for improving defense acquisition and procurement. Acquisition planning and management involves many decision-making and action-taking processes that cover a complex environment including actual acquisition, contracting, fiscal, legal, personnel, and regulatory requirements. A sound decision-making process has to rely on data—high quality data. Often the available data is dirty, outdated, incomplete, or insufficient for the expert to make a decision. On the other hand, there are enormous amounts of data on the web that can be utilized to crystalize the needed information.

The paper will investigate how to leverage the information in public data sources to complement the internal data in order to support effective acquisition planning and management. The research is based on publicly accessible government acquisition databases at usaspending.gov and fpds.gov. Both databases host federal spending data from the last two decades and contain millions of records with detailed information about each contract. These rich repositories of data provide a great opportunity for us to learn from the past practices, and, hopefully, to gain some insights that can help us design better strategies for managing future projects.

A preliminary study showed that the acquisition data suffer from the quality problems as do all other real-world data. To achieve high quality data analytics, we have to improve the quality of data. Our previous research demonstrated the feasibility of using online information from reputable sources to fill the missing values and correct erroneous or inconsistent data of acquisition databases. The research in this paper takes that a step further. It aims to enhance the acquisition data with online information so as to discover patterns that otherwise would not be able to be found.

Trust is a key issue for using online data. In fact, the web has not only changed our ways of sharing and seeking information, it has also altered traditional notions of trust due to the fact that the information can be published anywhere by anyone for any purpose, and there is no authority to certify the correctness of the information. It is often up to the information consumers to make their own judgement about the credibility and accuracy of information they encountered online. Unfortunately, in the world nowadays, people are flooded with fake news and internet scams. Thus it becomes even harder for an information seeker to discriminate between true and false information. To make the situation even worse, even when data are deemed trustworthy, assessing the data quality in this big data era still brings many challenges. First, the diversity of data sources brings abundant data types and complex data structures and increases the difficulty of data integration. Second, data change very fast and the timeliness of data is very short, which necessitates higher requirements for processing technology (Cai & Zhu, 2015).

This paper explores only the usage of information from credible and reputable sources to enhance the data analytics ability. However, investigating appropriate methods to assess web data quality, to identify and acquire credible and accurate information will be one of our future research topics.

Research Methodology

The research work follows the Data Enhancement and Analytics System framework shown as Figure 1 (Wu, Tudoreanu, & Wang, 2018).

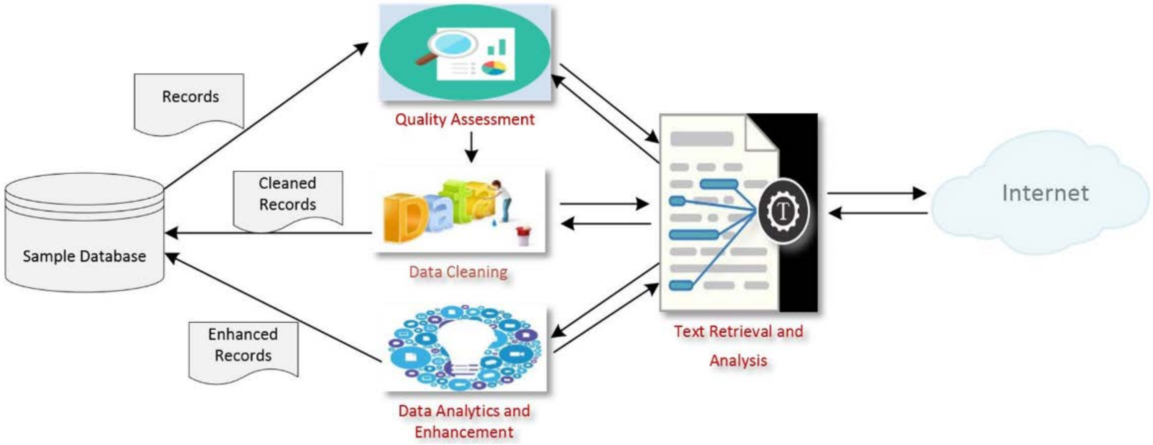


Figure 1. **Framework of Data Enhancement and Analytics System**

Our research methodology contains the following steps:

- Compare the data between fpds.gov and usaspending.gov in terms of their structures, contents, and quality.
- Apply data analytics techniques to discover patterns about past acquisition projects. These patterns might help us to identify the room for improvement in future projects.

Comparison of FPDS and USASPENDING Data

Both usaspending.gov and fpds.gov sites are publicly accessible and have the contract information of all U.S. departments since 2000; however, the data in two sites are organized in different structures with a different number of attributes. The data in usaspending.gov are categorized under prime award and sub-award. The types of spending include contracts, grants, loans, and other financial assistance. For each spending type, the data is organized into two structures: prime award and sub-award. For example, information on contracts is organized into two tables: one for prime contracts and the other for sub contracts. Data in fpds.gov is organized using a unified structure. We downloaded the spending data of the Department of Defense and stored them on a MYSQL database server.

Table 1 shows the structure of tables from each website, where the fpds row is from fpds.gov, and the other rows are from usaspending.gov. Here, RecCnt and ColCnt represent the number of records and number of columns in a table respectively; CompleteCols and SingleValCols represent the number of columns with no missing values and number of columns with only a single value across all records; and EmptyCols and IncompleteCols represent the number of empty columns and the number of columns with missing values respectively.

Table 1. Profiling of FPDS and usaspending Tables

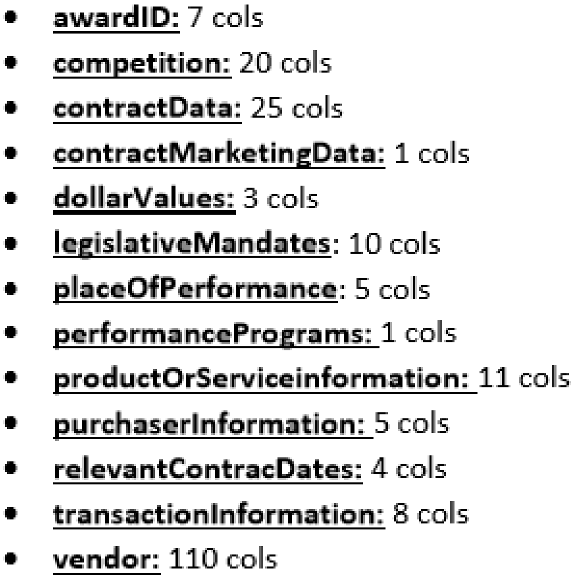
Table Name	ColCnt	CompleteCols/ SingleValCols	EmtpyCols	IncompleteCols
PrimeContracts	221	50/1	0	162
SubContracts	101	41/0	3	57
PrimGrants	67	32/5	2	33
SubAGrants	101	29/4	25	47
fpds	210	74/3	1	136

A close study of these tables reveals that the fpds table is similar to the PrimeContracts table from usaspending.gov in terms of their contents. Thus, the remaining part of this section compares only these two tables in terms of their schema, data coverage, and quality.

To facilitate the data comparison, attributes are classified into two categories: identity attributes and non-identity attributes. Identity attributes provide identity information for a contractor, contract, funding agency, etc. Examples of identity attributes include project identifier, contractor identifier (such as a DUNS number), business name, address information, phone, fax, etc. Non-identity attributes do not provide any identity information.

Attribute Naming Convention

PrimeContracts uses key description abbreviation to construct attribute names. Fpds groups attributes into categories. It then uses a key descriptor plus a category prefix to name an attribute. Compared to the PrimeContracts table, fpds attributes have longer but easy-to-understand names. The fpds attribute categories and the number attributes for each category are shown as in Figure 2.



- **awardID:** 7 cols
- **competition:** 20 cols
- **contractData:** 25 cols
- **contractMarketingData:** 1 cols
- **dollarValues:** 3 cols
- **legislativeMandates**: 10 cols
- **placeOfPerformance**: 5 cols
- **performancePrograms:** 1 cols
- **productOrServiceinformation:** 11 cols
- **purchaserInformation:** 5 cols
- **relevantContracDates:** 4 cols
- **transactionInformation:** 8 cols
- **vendor:** 110 cols

Figure 2. FPDS Attribute Categories

Schema Mapping

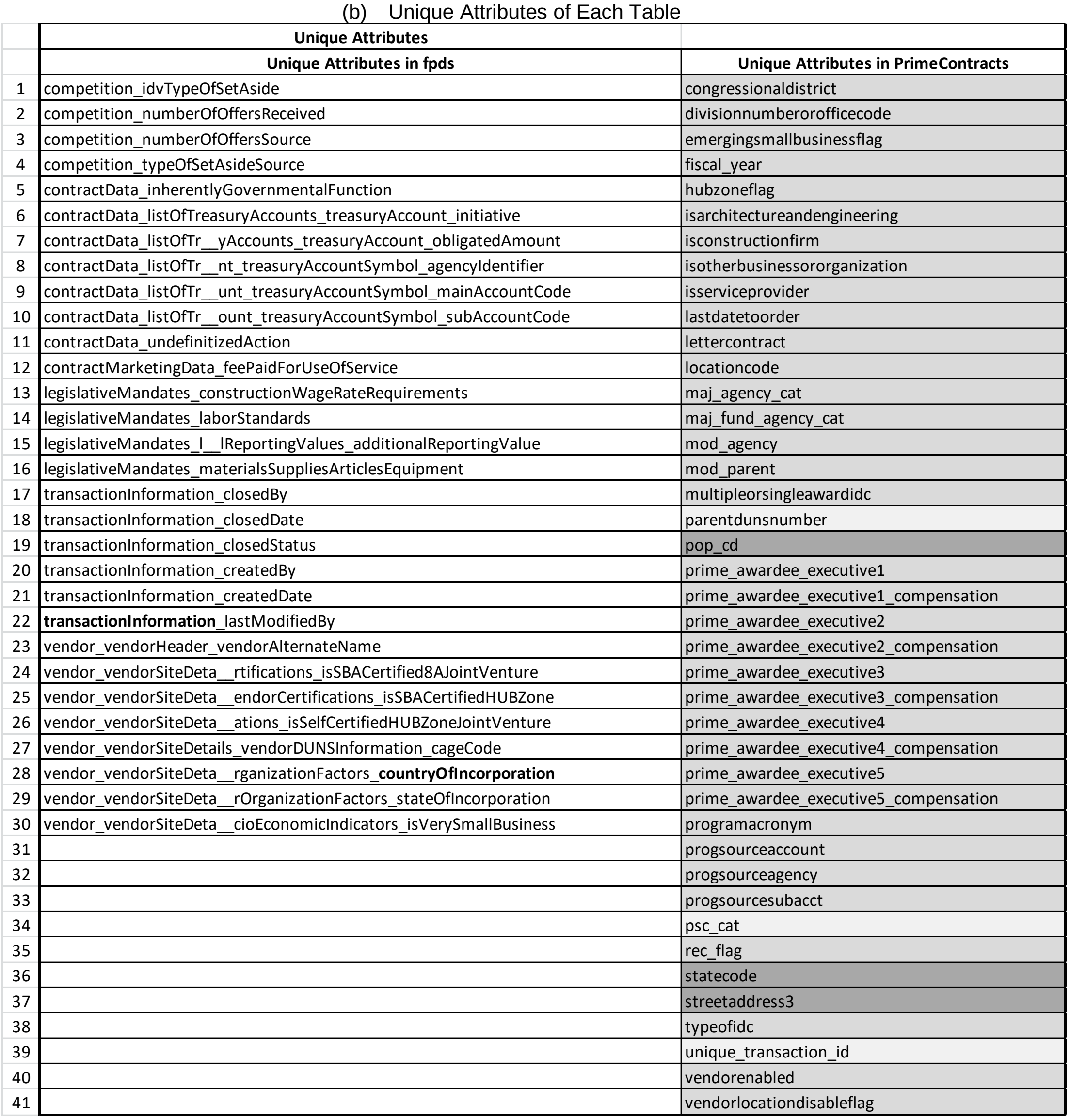
Schema mapping between the two tables are performed manually based on the data dictionary provided by each database. There are 180 common fields in the two tables even though these fields are named differently in each table. The remaining 30 attributes in fpds and 41 attributes in PrimeContracts are found only in their own table. Due to space limitations, Table 2 only shows the partial mapping results.

Table 2. Schema Mapping Between fpds and PrimeContracts Tables

(a) Mapping of Common Attributes

	Mapping Attributes	
	Attributes in fpds	**Matched Attributes in PrimeContracts**
1	awardID_awardContractID_PIID	piid
2	awardID_awardContractID_agencyID	agencyid
3	awardID_awardContractID_modNumber	modnumber
4	awardID_awardContractID_transactionNumber	transactionnumber
5	awardID_referencedIDVID_PIID	idvpiid
6	awardID_referencedIDVID_agencyID	idvagencyid
7	awardID_referencedIDVID_modNumber	idvmodificationnumber
8	competition_A76Action	a76action
9	competition_commercialItemAcquisitionProcedures	commercialitemacquisitionprocedures
10	competition_commercialItemTestProgram	commercialitemtestprogram
11	competition_competitiveProcedures	competitiveprocedures
12	competition_evaluatedPreference	evaluatedpreference
13	competition_extentCompeted	extentcompeted
14	competition_fedBizOpps	fedbizopps
15	competition_idvNumberOfOffersReceived	numberofoffersreceived
	……	**……**
	……	**……**
165	vendor_vendorSiteDeta__ndorSocioEconomicIndicators_isIndianTribe	isindiantribe
166	vendor_vendorSiteDeta__allyDisadvantagedWomenOwnedSmallBusiness2	isecondisadvwomenownedsmallbusiness
167	vendor_vendorSiteDeta__ors_isJointVentureWomenOwnedSmallBusiness	isjointventurewomenownedsmallbusiness
168	vendor_vendorSiteDeta__s_isNativeHawaiianOwnedOrganizationOrFirm	isnativehawaiianownedorganizationorfirm
169	vendor_vendorSiteDeta__erviceRelatedDisabledVeteranOwnedBusiness	srdvobflag
170	vendor_vendorSiteDeta__cioEconomicIndicators_isTribally OwnedFirm	istribally ownedfirm
171	vendor_vendorSiteDeta__dorSocioEconomicIndicators_isVeteranOwned	veteranownedflag
172	vendor_vendorSiteDeta__endorSocioEconomicIndicators_isWomenOwned	womenownedflag
173	vendor_vendorSiteDeta__nomicIndicators_isWomenOwnedSmallBusiness	iswomenownedsmallbusiness
174	vendor_vendorSiteDeta__Owned_isAsianPacificAmericanOwnedBusiness	apaobflag
175	vendor_vendorSiteDeta__inorityOwned_isBlackAmericanOwnedBusiness	baobflag
176	vendor_vendorSiteDeta__rityOwned_isHispanicAmericanOwnedBusiness	haobflag
177	vendor_vendorSiteDeta__cIndicators_minorityOwned_isMinorityOwned	minorityownedbusinessflag
178	vendor_vendorSiteDeta__norityOwned_isNativeAmericanOwnedBusiness	naobflag
179	vendor_vendorSiteDeta__cators_minorityOwned_isOtherMinorityOwned	isotherminorityowned
180	vendor_vendorSiteDeta___isSubContinentAsianAmericanOwnedBusiness	saaobflag

(b) Unique Attributes of Each Table



	Unique Attributes	
	Unique Attributes in fpds	**Unique Attributes in PrimeContracts**
1	competition_idvTypeOfSetAside	congressionaldistrict
2	competition_numberOfOffersReceived	divisionnumberorofficecode
3	competition_numberOfOffersSource	emergingsmallbusinessflag
4	competition_typeOfSetAsideSource	fiscal_year
5	contractData_inherentlyGovernmentalFunction	hubzoneflag
6	contractData_listOfTreasuryAccounts_treasuryAccount_initiative	isarchitectureandengineering
7	contractData_listOfTr__yAccounts_treasuryAccount_obligatedAmount	isconstructionfirm
8	contractData_listOfTr__nt_treasuryAccountSymbol_agencyIdentifier	isotherbusinessororganization
9	contractData_listOfTr__unt_treasuryAccountSymbol_mainAccountCode	isserviceprovider
10	contractData_listOfTr__ount_treasuryAccountSymbol_subAccountCode	lastdatetoorder
11	contractData_undefinitizedAction	lettercontract
12	contractMarketingData_feePaidForUseOfService	locationcode
13	legislativeMandates_constructionWageRateRequirements	maj_agency_cat
14	legislativeMandates_laborStandards	maj_fund_agency_cat
15	legislativeMandates_l__lReportingValues_additionalReportingValue	mod_agency
16	legislativeMandates_materialsSuppliesArticlesEquipment	mod_parent
17	transactionInformation_closedBy	multipleorsingleawardidc
18	transactionInformation_closedDate	parentdunsnumber
19	transactionInformation_closedStatus	pop_cd
20	transactionInformation_createdBy	prime_awardee_executive1
21	transactionInformation_createdDate	prime_awardee_executive1_compensation
22	**transactionInformation**_lastModifiedBy	prime_awardee_executive2
23	vendor_vendorHeader_vendorAlternateName	prime_awardee_executive2_compensation
24	vendor_vendorSiteDeta__rtifications_isSBACertified8AJointVenture	prime_awardee_executive3
25	vendor_vendorSiteDeta__endorCertifications_isSBACertifiedHUBZone	prime_awardee_executive3_compensation
26	vendor_vendorSiteDeta__ations_isSelfCertifiedHUBZoneJointVenture	prime_awardee_executive4
27	vendor_vendorSiteDetails_vendorDUNSInformation_cageCode	prime_awardee_executive4_compensation
28	vendor_vendorSiteDeta__rganizationFactors_**countryOfIncorporation**	prime_awardee_executive5
29	vendor_vendorSiteDeta__rOrganizationFactors_stateOfIncorporation	prime_awardee_executive5_compensation
30	vendor_vendorSiteDeta__cioEconomicIndicators_isVerySmallBusiness	programacronym
31		progsourceaccount
32		progsourceagency
33		progsourcesubacct
34		psc_cat
35		rec_flag
36		statecode
37		streetaddress3
38		typeofidc
39		unique_transaction_id
40		vendorenabled
41		vendorlocationdisableflag

Quality Assessment

Due to the space limitation, only the quality assessment of key identity attributes is presented here. Quality assessment is performed on the dimensions of column completeness, and field length consistency of attributes that have fixed-length values. Table 3 shows that the fpds table has a higher column completeness measure than the PrimeContracts table. Figures 3 and 4 show the field length distribution of the PIID (prime project ID) and prime contractor DUNS numbers respectively. Since the PIID is a system wide identifier for each prime project, it is assumed to have a fixed length. But there are some exceptions in both the fpds and PrimeContract tables. Similarly, the DUNs number is a 9-digit value. Any DUNS numbers other than 9-digit are considered incorrect.

Table 3. Column Completeness

Table Name	ColCnt	IncompleteCols	%CompleteCols
PrimeContracts	212	162	23.6%
fpds	210	136	35.2%

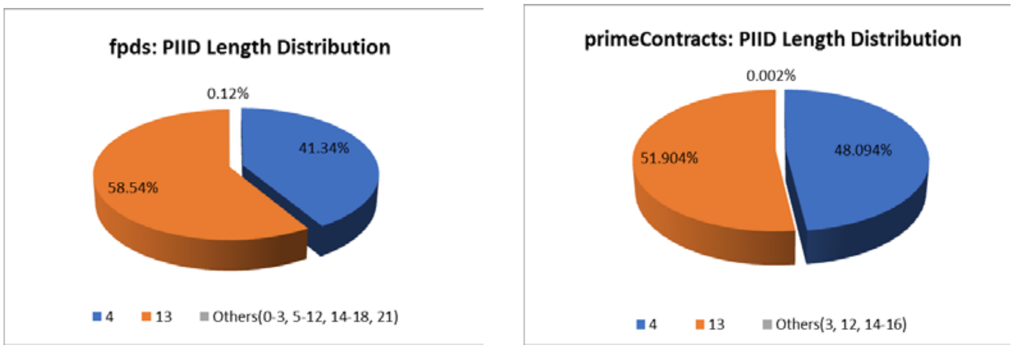


Figure 2. **PIID Length Distribution**

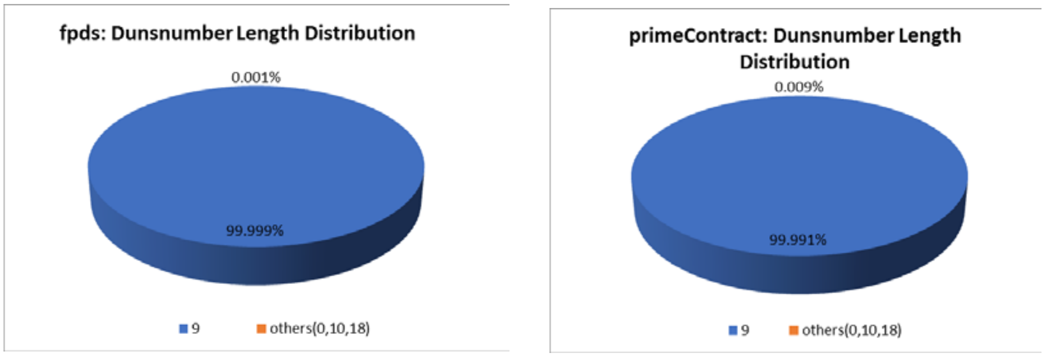


Figure 3. **DUNs Number Length Distribution**

Record Mapping

Record mapping matches records of the two tables if they represent the same entity. In fpds and PrimeContracts, each contract is considered as an entity. Since both tables contain the contract information from the Department of Defense, record mapping provides a way to measure the data consistency between them. Record mapping is a typical entity resolution process. It requires comparing fields of records to determine whether they belong to the same entity or not. If records have common key identifier attributes, mapping them is rather straightforward; otherwise, the non-identifier attributes have to be used to determine how similar the records are. Unfortunately, the fpds and PrimeContracts tables don't have a common record identifier, thus record mapping must rely on the common attributes of two tables.

Considering the number of attributes and records in the fpds and PrimeContracts tables, record mapping is a very complicated and time-consuming process. Thus, the first phase of mapping is performed on sample data instead, and it considers only the following identity attributes when matching records: PIID, dunsnumber, vnedorlocationzipcode, vendorlocationstate, vendorlocationcity, vendor_countrycode, vendor_phoneno, and vendorlocation_streetaddress. Here, PIID denotes the primary project ID that is unique to each project. Dunsnumer denotes the 9-digit DUNS number of the primary contractor of a project. vnedorlocationzipcode, vendorlocationstate, vendorlocationcity, vendor_countrycode, vendor_phoneno, and vendorlocation_streetaddress represent address and telephone information of a primary contractor. Two records are considered to represent the same entity if their values on each of the above attributes match.

The following steps are performed to prepare the sample datasets:

- A random sample of 5000 PIIDs that exist in both tables is drawn.

- The corresponding records of these PIIDs are retrieved from the fpds and PrimeContract tables respectively and they are stored into separate datasets, denoted as datasets D_f, and D_u.
- As data quality issues will adversely affect the record matching result, data standardization and transformation are performed. Duplicate records and records with missing values are removed.
- The equijoin is applied on two datasets, and the resulting dataset is denoted as D_{join}.

Figure 4 compares the number of distinct values of each identity attribute among three datasets D_f, D_u, and D_{join}. It shows that D_u consistently has more distinct values for each attribute than D_f. The number of distinct values for each attribute in table D_{join} indicates the number of attribute common values between D_f and D_u.

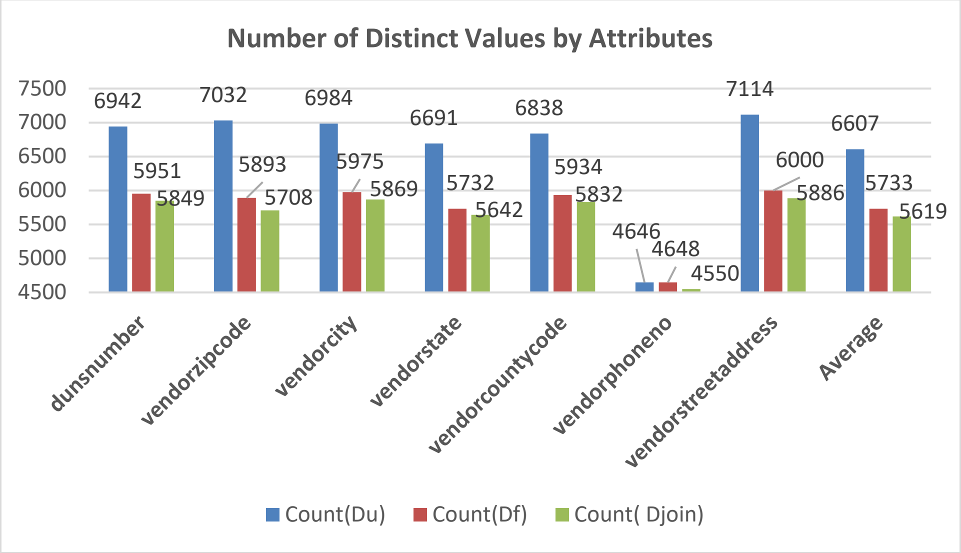


Figure 4. **Number of Distinct Values by Attributes**

Figure 5 shows the relative consistency measure of each attribute of one table in terms of the other table. For example, 98.3% of dunsnumbers in D_f are also found in D_u, while only 84.3% of dunsnumber in D_u are found in D_f; 96.7% of vendorzipcodes in D_f are also found in D_u, but 81.2% of vendorzipcodes in D_u are found in D_f. The reason behind these discrepancies is that, given a prime award ID, there are more distinct records in D_u than in D_f. Possible root causes may include the following: fpds.gov and usaspending.gov collected the data at different granularity levels, the fpds database may miss some records, or the usaspending database may have to keep multiple records for the same prime award as these records have inconsistent values and it is not clear which values are right and which are not.

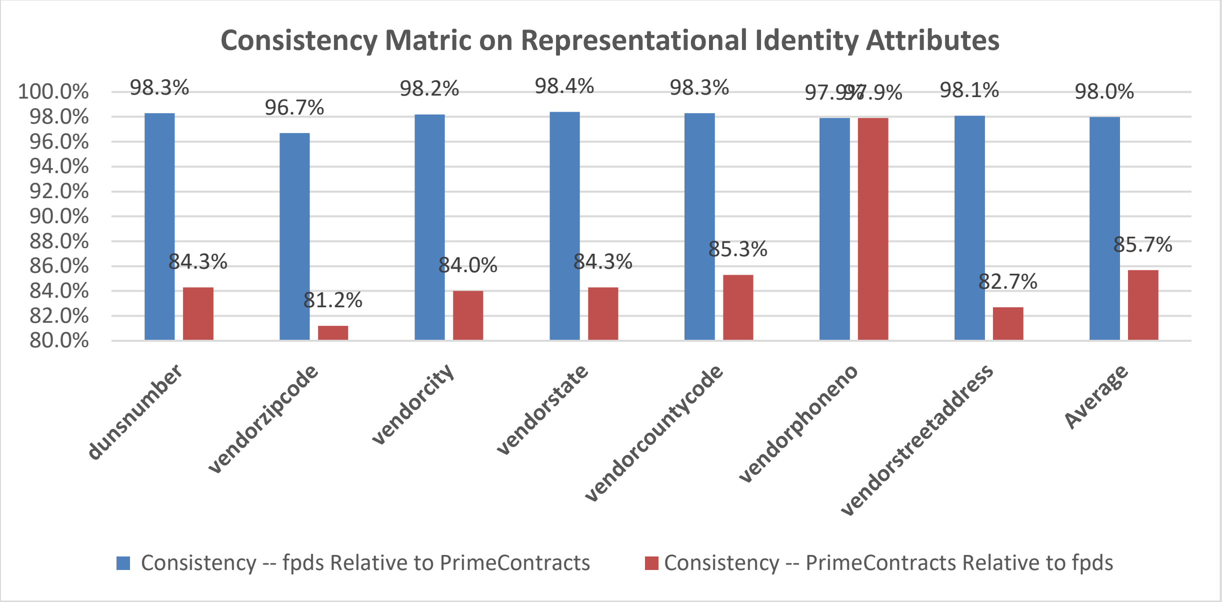


Figure 5. **Relative Consistency Measure of Each Attribute**

Data Analytics

The goal of data analytics is to discover hidden and interesting patterns that can be potentially useful in planning future acquisition projects. Since we are not the domain expert on acquisition data and policies, we decide to take data science approach and start the data analytics with a hypothesis.

Hypothesis 1: Critical contractors are those that provide unique products and services. They could be the weakest link in a supply chain, because if they failed, it would be hard to find alternatives to fill their places.

North American Industry Classification System (NAICS) is the standard used by federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy. NAICS code describes the business specialization of a company.

There are 379 distinct NAICS codes among all contractors. Seventy-eight NAICS codes have only one contractor associated with it. This means in the current pool of DoD contractors, these 78 contractors are critical contractors as no other DoD contractors are doing the same business. It is possible that there are companies that, outside the DoD contractor pool, are associated with these NAICS codes. On average, each of those critical contractors is involved in 37 different projects. The top 10 critical contractors with the most number of projects is listed in Table 4.

Table 4. The Top 10 Critical Contractors With the Most Number of Projects

Rank	No. of Distinct Projects
1	399
2	382
3	343
4	245
5	237
6	138
7	117
8	91
9	69
10	61

For those highly demanded contractors, most of them are big and well-established companies, but a couple of them are small companies that appear to provide very unique products and services. These companies could be a potential weak point in a project/supply chain and may critically affected the overall outcome of a project if they fail.

Hypothesis 2: A primary project usually has hundreds of contractors working on it. These contractors spread out in different geographical locations. Some may be located in an area with a high risk of natural disasters such as earthquakes, flooding, hurricanes, tornados, and so forth. Some natural disasters, like tornados and earthquakes, are hard to predict. Thus, it would be always beneficial to consider those risk factors when planning a project. Possible strategies include using contractors located in low-risk areas, or intentionally selecting contractors that are spread out in different geographical locations, or having backup plans in place to handle any emergencies.

We have obtained the natural disaster data for each U.S. county between the years 1950 and 2018 from the National Centers for Environmental Information (Formerly the National Climatic Data Center [NCDC]). The data cover all types of natural disasters, including floods, tornados, hurricanes, blizzards, high winds, flash floods, hail, dust storms, and so forth.

This project focuses on disasters that could cause severe damages and significantly affect the normal life and business operations of local communities such as tornados, hurricanes, floods, and blizzards. Since the world weather has changed quite fast in recent decades, we decided to use the NCDC data of last 20 years to identify whether an area is prone to a natural disaster based on the following criteria. The high-risk flooding areas are identified as those that have at least 10 episodes of floods in the last 20 years; the high-risk hurricane areas are those that have at least one hurricane in last 20 years; the high-risk wildfire areas are those that have at least one wildfire that lasted more than one day in last 20 years; and the high-risk tornado areas are those that have at least one category 3 or above tornado in the last 20 years. Table 5 shows the number of subcontractor zip codes belong to each disaster type.

Table 5. Number of Subcontractor Zip Codes Vulnerable to Each Disaster Type

Disaster Type	Flood	Hurricane	Tornado	Wildfire
# zipcodes	5959	780	1182	1831

Our analysis found that there are 6,786 natural disaster–prone zip codes of the principal places where the work is performed for a subcontract. Some of these zip codes are vulnerable to more than one disaster type. The natural disaster–prone areas are further categorized into four classes based on the number of distinct disaster types that has been observed in that area during the last 20 years.

Table 6 shows the distribution of subcontract principal place zip by the number of disaster types along with the distribution of subcontractors located in those zip codes. The column %zip_population indicates the percentage of zip codes (of a category) with regard to the total number of subcontract zip codes, and %DUNS_population indicates the percentage of DUNs in each category of zips with regard to total number of subcontractor DUNS number.

Table 6. Distribution of Subcontractor Principal Zip and DUNS

#DisasterTypes	#zipcodes	%zip_population	#duns	% DUNS_population
1	2165	7.8%	13373	42.3%
2	3548	12.9%	10965	34.6%
3	1004	3.6%	2733	8.6%
4	69	0.25%	141	0.44%
Total:	6786	23.7%	27072	86.0%

Subcontractors that are located in an area vulnerable to all four disaster types are considered to have a high risk. Table 7 shows the top 10 projects with the highest number of high-risk contractors.

Table 7. Top 10 Projects With the Highest Number of High-Risk Contractors

Rank	No. of High-Risk Contractors
1	59
2	49
3	43
4	37
5	36
6	31
7	27
8	24
9	23
10	19

It would be interesting to know the percentage of high-risk contractors in past projects. There are total 588 projects have at least one high-risk subcontractors. Figure 6 shows the distribution of projects by their percentage of contractors that are vulnerable to all four types of natural disaster. A close study reveals that the majority of 129 projects in the last bin with more than 90% of subcontractors in high-risk areas have only one subcontractor. More than half of 588 projects have less than 10% of subcontractors in high-risk areas. Ideally, a project should have as few as possible high-risk subcontractors.

We believe the information on high-risk areas of natural disasters is beneficial because it helps project managers calculate the risk of a project and develop strategies to mitigate the risk to the minimum.

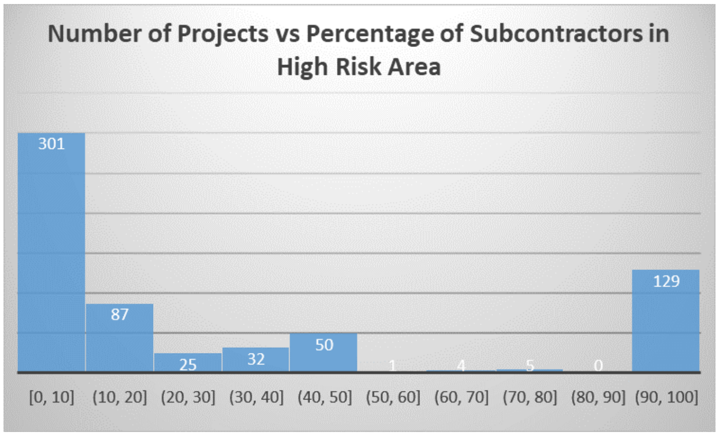


Figure 6. **Distribution of Projects by Percentage of High-Risk Subcontractors**

Related Work

This section summarizes some related work in the fields of federal acquisition data analysis.

Tudoreanu et al. (2018) investigated employment data in an attempt to correlate changes in employment with negative modifications to contracts. Such correlations can be explored to infer hidden and undisclosed contractors. Hidden contractors may pose the risk of becoming a weak, stress point of a project and would affect the overall outcome of the project.

Wu et al. (2018) proposed a framework based on data science approach that aims to utilize the online information to assess and improve acquisition database quality as well as to find the hidden patterns to further acquisition research. The main component of the framework is a web-search and text mining module, whose main function is to search the internet and identify the most credible and accurate information online.

Apte, Rendon, and Dixon (2015) explored the use of Big Data analytic techniques to explore and analyze large dataset that are used to capture information about DoD services acquisitions. The paper described how big data analytics could potentially be used in acquisition research. As the proof of concept, the paper tested the application of Big Data Analytic techniques by applying them to a dataset of Contractor Performance Assessment Report System (CPARS) ratings of 715 acquired services. It also created predictive models to explore the causes of failed services contracts. Since the dataset used in the research was rather small and far from the scope of big data, the techniques explored by the paper mainly focus on traditional data mining techniques without taking into account big data properties.

Black, Henley, and Clute (2014) studied the quality of narratives in CPARS and their value to the acquisition process. The research used statistical analysis to examine 715 Army service contractor performance reports in CPARS in order to understand three major questions: (1) To what degree are government contracting professionals submitting to CPARS contractor performance narratives in accordance with the guidelines provided in the CPARS user's manual? (2) What is the added value of the contractor performance narratives beyond the value of the objective scores for performance? (3) What is the statistical relationship between the sentiment contained in the narratives and the objective scores for contractor evaluations?

Conclusion and Future Work

This research presented a data science approach to compare and analyze publicly accessible acquisition databases. The research explored the usage of online information to enhance the internal data in order to discover the hidden patterns in the data. The research has collected natural disaster information from the National Centers for Environmental Information. This information can be helpful in identifying high-risk locations and contractors located in those locations.

Future work will focus on the following two directions. First, explore more data analytics techniques to discover patterns that are potentially useful to the acquisition research community. Second, research effective text mining techniques for assessing web data quality and retrieving credible information from online sources.

References

Apte, U., Rendon, R., & Dixon, M. (2016). Big data analysis of contractor performance information for service acquisition in DoD: A proof of concept. In *Proceedings of the 13th Annual Acquisition Research Symposium*. Monterey, CA: Naval Postgraduate School.

Augustine, N. R. (1997). *Augustine's laws*. AIAA.

Black, S., Henley, J., & Clute, M. (2014). *Determining the value of Contractor Performance Assessment Reporting System (CPARS) narratives for the acquisition process* (NPS-CM-14-022). Monterey, CA: Naval Postgraduate School.

Brown, B. (2010). *Introduction to defense acquisitions management.* Fort Belvoir: VA: Defense Acquisition University. Retrieved from www.dau.mil/publications/publicationsDocs/Intro%20to%20Def%20Acq%20Mgmt%2010%20ed.pdf

Cai, L., & Zhu, Y. (2015). The challenges of data quality and data quality assessment in the big data era. *Data Science Journal, 14*, 2. doi: http://doi.org/10.5334/dsj-2015-002

Cheskin, S. (1999). *Ecommerce trust: Building trust in digital environments*. Archetype/Sapient.

Cilli, M., Parnell, G. S., Cloutier, R., & Zigh, T. (2015). A systems engineering perspective on the revised defense acquisition system. *Systems Engineering, 18*(6), 584–603. doi:10.1002/sys.21329.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, *58*(6), 737–758.

DAU. (n.d.). DAU Center for Defense Acquisition Research agenda 2016–2017. Retrieved from http://dau.dodlive.mil/files/2016/01/ARJ-76_ONLINE-FULL.pdf

DoD. (2007, November). *Operation of the Defense Acquisition System* (DoDI 5000.01). Washington, DC: Author.

DoD. (2015). *Operation of the Defense Acquisition System* (DoDI 5000.02). Washington, DC: Author.

Fogg, B. J., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N., … Treinen, M. (2001). What makes web sites credible?: A report on a large quantitative study. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 61–68). New York, NY: ACM Press.

Gallup et al. (2015, May). Lexical Link Analysis (LLA) application: Improving web service to defense acquisition visibility environment. *Distributed Information Systems Experimentation*.

Gaither, C. C. (2014). Incorporating market based decision making processes in defense acquisitions. *International Journal of Defense Acquisition Management, 6*, 38–50.

Golbeck, J. (2008). Trust on the world wide web: A survey. *Foundations and Trends® in Web Science, 1*(2), 131–197.

Hagan, G. (1998). *Glossary: Defense acquisition acronyms and terms*. Fort Belvoir, VA: DoD, Defense Systems Management College, Acquisition Policy Department.

Krzysko, M. (2012, February). The need for acquisition visibility. *Journal of Software Technology*, 4–9.

Krzysko, M. (2016). *Acquisition decision making through information and data management.* Retrieved from www.digitalgovernment.com/media/Downloads/asset_upload_file917_5737.pdf

McKernan, M., Moore, N. Y., Connor, K., Chenoweth, M. E., Drezner, J. A., Dryden, J., … Szafran, A. (2016). *Issues with access to acquisition and information in the Department of Defense.* Santa Monica, CA: Rand Corporation.

Metzger, M. J., & Flanagin, A. J. (2013). Credibility and trust of information in online environments: The use of cognitive heuristics. *Journal of Pragmatics, 59*, 210–220.

Miller, A., & Ray, J. (2015, January). Moving from standard practices to best practices in defense acquisition. *Defense ARJ, 22*(1), 64–83.

Pennock, M. J. (2008). Defense acquisition: A tragedy of the commons. Retrieved from *ProQuest*.

Tudoreanu, M. E., Franklin, K., Wu, N., & Wang, R. (2018). Searching hidden links: Inferring undisclosed subcontractors from public contract records and employment data. In *Proceedings of the 15th Annual Acquisition Research Symposium*. Monterey, CA: Naval Postgraduate School.

Wu, N., Tudoreanu, M. E., & Wang, R. (2018). Leveraging public data for quality improvement and pattern discovery of federal acquisition data. In *Proceedings of the 15th Annual Acquisition Research Symposium*. Monterey, CA: Naval Postgraduate School.

Identification and Characterization of Data for Acquisition Category (ACAT) II–IV Programs

Megan McKernan—is a Senior Defense Researcher at RAND. She has more than 14 years of experience conducting DoD acquisition analyses. She is co-leading research examining DoD acquisition data management. She has also conducted other defense acquisition analyses: prototyping, IT acquisition, Industrial Base considerations, tailoring the acquisition process, program manager tenure, and root causes of Nunn-McCurdy unit cost breaches. She uses a variety of methods in conducting research including case studies, interviews, and literature reviews. She holds an MA in international trade and investment policy from the George Washington University and a BA in economics from William Smith College. [mckernan@rand.org]

Jeffrey A. Drezner—is a Senior Policy Researcher at RAND. He has over 34 years of professional experience conducting policy analysis on a wide range of issues, including planning and program management, analyses of cost and schedule outcomes in complex system development programs, aerospace industrial policy, and defense acquisition policy and reform. His research continues to emphasize mixed qualitative and quantitative approaches to analyze issues associated with technology development, organizational behavior, and program management. Drezner received his PhD in political science from Claremont Graduate University. [zner@rand.org]

Abstract

Acquisition data lay the foundation for decision-making, management, insight, and oversight of the Department of Defense's (DoD's) acquisition program portfolio. A large amount of information—based on statutory and regulatory reporting requirements and used for program execution, oversight, insight, and analysis—is collected on the higher cost major defense acquisition programs (MDAPs; referred to as Acquisition Category [ACAT] I programs). However, the DoD also makes additional smaller investments that are categorized as ACAT II–IV acquisition programs, pre-MDAPs, and Defense Business Systems, and the current program data environment features varying definitions, policy, collection methods, and use cases across the DoD. RAND researchers documented the DoD status quo for identifying, collecting, and storing acquisition data from different programs, performed an initial gap analysis, and developed recommendations that build on what the OSD and Service acquisition information managers have accomplished to date and that move the DoD toward a common framework for data governance and management.

Introduction

Acquisition data lay the foundation for decision-making, management, and oversight of the Department of Defense's (DoD's) weapon system acquisition portfolio. This information is collected to meet statutory and regulatory reporting requirements and to support program execution, insight, oversight, and analysis. The DoD groups its acquisition programs into categories. Acquisition categories (ACATs) refer to dollar values of the investment,[1] and ACAT I programs cost the most (DoD, 2017).[2] According to the U.S. Government Accountability Office (GAO, 2015, p. 1),

[1] At the time of this writing (October 2018), there was some debate within the DoD over whether Middle Tier acquisition programs have ACAT levels. Middle Tier programs are new, so the specifics are still being worked out.

[2] According to DoD (2017, p. 28), Dollar value for all increments of the [ACAT I] program: estimated by the [Defense Acquisition Executive] DAE to require an eventual total expenditure for research, development, and test and evaluation (RDT&E) of more than $480 million in Fiscal Year (FY) 2014 constant dollars or, for procurement, of more than $2.79 billion in FY 2014 constant dollars.

> In Fiscal Year 2014, DoD requested $168 billion to develop, test, and acquire weapon systems and other products and equipment. About 40 percent of that total was for major defense acquisition programs (MDAP) or Acquisition Category (ACAT) I programs. The remaining approximately 60 percent of the budget request included, among other investments, funding for DoD's non-major ACAT II and III programs.

The GAO has documented the challenges of gaining insight into ACAT II–IV in a 2015 report (GAO, 2015).

The Office of the Secretary of Defense asked the RAND Corporation National Defense Research Institute to document the DoD's status quo for identifying, collecting, and storing ACAT II–IV acquisition programs, then perform an initial gap analysis and recommend actions that could move the DoD toward a common framework for acquisition program data. This analysis builds on four earlier studies on *Issues with Access to Acquisition Data and Information in the Department of Defense* (Riposo et al., 2015; McKernan et al., 2016; McKernan et al., 2017; McKernan et al., 2018). This report should be of interest to government acquisition professionals, oversight organizations, and, especially, the analytic community. This research was sponsored by the Office of the Secretary of Defense[3] and conducted within the Acquisition and Technology Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community. For more information on the RAND Acquisition and Technology Policy Center, see http://www.rand.org/nsrd/about/atp.html or contact the director (contact information is provided on the webpage).

The DoD Lacks Visibility Into ACAT II–IV Acquisition Programs

In response to a GAO question, DoD senior leadership asked staff to examine the performance of ACAT II–IV programs. The program data required to perform this analysis was not readily available. As one step in meeting this information need, the Acquisition Data office within the Office of the Under Secretary of Defense for Acquisition and Sustainment has been working with the Services over the past few years to track and collect ACAT II–IV program information more efficiently.[4] Challenges include the scarcity of data on lower ACAT programs; the inconsistency of the ACAT II–IV data that are collected at the Office of the Secretary of Defense (OSD) and Component Acquisition Executive (CAE) levels; and the question of what kind of oversight makes sense for ACAT II–IV programs to ensure that proper management oversight, portfolio analyses, and other assistance is available while minimizing the burden on program managers (PMs). The challenges of gaining insight into ACAT II and III programs are described in the 2015 GAO report, which concludes that the DoD cannot provide reliable data on the number, cost, or performance of ACAT II and III programs (GAO, 2015, p. 6).

The current program data environment as described here features varying definitions, policy, collection methods, and use cases across the Components and the OSD. The result is that basic questions (e.g., How many programs are in each Component?) cannot be easily and consistently answered, and the DoD lacks the ability to understand trends and program execution

These thresholds are for ACAT I programs but are not applicable for ACAT IA programs.

[3] This study was commissioned by Mark Krzysko, Director, Acquisition Data, within the Office of the Under Secretary of Defense for Acquisition and Sustainment.

[4] The prior name of this organization was Acquisition Resources and Analysis, Enterprise Information within the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.

status at an aggregate level for these portfolios. The program data environment also has little coordination across Components and the OSD except through largely ad hoc interactions of acquisition information managers in each organization. However, some level of basic agreement exists on a core set of data, particularly at the ACAT I level, and the need for quality data suitable for a variety of use cases remains constant, along with a colloquially expressed data management goal to "enter once, use many."

Congressional interest in this area has increased over the past several years. Recent NDAAs recognize the potential benefits of a common data framework and environment. As of late 2018, the DoD does not know exactly how far away it is from a common acquisition data framework; however, the organization does have an understanding of some of the actions that need to occur and has taken definitive steps to move toward a common data framework for acquisition program data. The Office of the Under Secretary of Defense asked the RAND Corporation to identify how the OSD and the Components go about collecting program data, then perform an initial gap analysis and recommend actions that could move the DoD toward a common framework for acquisition program data.

Our approach for this study included analyzing current policy in the OSD and the Services and holding discussions with subject-matter experts throughout the DoD to understand the policy and data frameworks for ACAT I–IV programs. We also collected information on ACAT I as a benchmark for comparison because ACAT I programs have a well-established data framework, developed through use over several decades and reflecting agreement between the OSD and the Services.

Key Findings

The OSD and the Services have created procedures that in effect align the collection and transmission of data with OSD and congressional information requirements, and use formal communication mechanisms (e.g., the Acquisition Visibility Working Group [AVWG] and the Acquisition Visibility Steering Group [AVSG]) as instruments to help standardize and talk through information management challenges. The OSD and the Services have also recently created an Acquisition Program List (APL) that consolidates Service-level lists of ACAT programs in one location in the OSD's Defense Acquisition Visibility Environment (DAVE). The U.S. Navy and the U.S. Air Force (USAF) currently use mixed methods in which some data are digitally pushed to DAMIR and other data are input manually. The Army manually inputs program data directly into DAMIR.

Overall, we found that the OSD and Service policy and data environments for ACAT programs are very similar. Based largely on ACAT I program statutory, regulatory, and policy information requirements, there appears to be a shared recognition that program data are required to support multiple use cases and a general agreement that program data include the same core information related to cost, schedule, performance, and risk.

Additionally, there appears to be a shared understanding of the definitions of those program data even as the specific metrics used and preferred by leadership in the OSD and the Services differ somewhat. Furthermore, the Services have created procedures that in effect align the collection and transmission of data with OSD information requirements. Within the past decade, the USAF and the Navy have intentionally aligned their centralized program information systems—Project Management Resource Tools (PMRT)[5] and Research, Development, and Acquisition

[5] PMRT's predecessor, the System Metric and Reporting Tool, was also used as part of the alignment.

Information System (RDAIS)—to the OSD's program information system, DAMIR. The Services have also moved toward closer collaboration with the OSD. The USAF and the Navy currently use a mixed method in which some data are digitally pushed to DAMIR by PMRT and RDAIS and other data are input manually. Currently, the Army manually inputs ACAT I program data directly into DAMIR in the absence of a centralized program information system within the Army. The movement of both the USAF and the Navy toward the use of "pushing" and "pulling" information between information systems is driven in part by the need to reduce the burden on program offices through sharing common information across a broad range of information requirements (i.e., enter once, use many) and also to achieve some efficiencies by taking advantage of improvements in technology. The convergence by the Services and the OSD on the limited common data framework as described has taken a considerable amount of effort, collaboration, and time (likely more than 10 years).

Our summary assessment of key attributes of the program data policy and management practice environment appears in the following list and in Table 1.

- **Information governance**. The policy environment for ACAT I program information is well established; the OSD and the Services have similar acquisition policy frameworks, including information governance for program data. The Services are responsible for promulgating policy for ACAT II–IV. For the most part, information governance for ACAT II–IV programs is similar to that of ACAT I.
- **Roles, responsibilities, and authorities**. Policy generally specifies acquisition-related roles, responsibilities, and authorities (RRA) for ACATs. Nevertheless, RRA are fairly consistent across the Services for ACAT programs of all levels with centralized authority (the Defense Acquisition Executive [DAE] or Service Acquisition Executive [SAE]) and decentralized responsibility for execution (program executive officers [PEOs] and PMs). Across program types and organizations, the program is responsible for collecting and reporting most program-level data.
- **Use cases**. Use cases are the demand signal for acquisition program data and often identify the data required, both explicitly and implicitly. The use cases for acquisition program data—program management and execution, oversight, statutory and regulatory reporting, and portfolio analyses—appear to be largely similar across the OSD and the Services and across ACAT levels.
- **Processes**. The milestone, event-driven acquisition process is well defined in policy and is fairly consistent in its attributes across organizations and ACAT levels. The process both generates program data through program execution and consumes program data in milestone decisions and technical reviews.
- **Authoritative data and definitions**. Best practices in data management assume that each unique data element (or data field) is identified and associated with a precise meaning or content. The OSD, the USAF, and the Navy have authoritative data fields defined in their information systems for ACAT I programs; the Air Force and the Navy carry those definitions down to the smaller ACAT II–IV programs. The OSD, the USAF, and the Navy also have data dictionaries available to system users. The Army inputs ACAT I program data manually into DAMIR, and ACAT II–III program data are captured in briefings that appear to follow a standard template. The Army also tracks basic information on ACAT II–III program data in the Army Acquisition Program Master List (AAPML), which resides in DAVE within the OSD. The AAPML provides basic counts of programs by level, phase, or Milestone Decision Authority (MDA). Apparent differences in specific data elements reported and the definitions of those data elements across the OSD, the Army, the Navy, and the USAF largely occur because the specific data elements and metrics reported are tailored to a particular organization's culture, its

historical precedents, and the preferences of that organization's current senior leadership (i.e., how the current leadership wishes to view the information for decision-making). The underlying data—the cost, schedule, performance, and risk information captured and reported at the program level—tend to be similar or the same. This consistency is partly because some data elements are defined in statute (e.g., unit cost).

- **Data, business, and system rules**. The Services have created procedures at the ACAT I level that, in effect, align the collection and transmission of data with the OSD requirements for program data and other acquisition information. In general, the rules underlying data definitions are present in data dictionaries for the OSD, the USAF, and the Navy (the organizations that have such dictionaries). However, rules underlying business processes and information systems are not explicitly stated in guidance or user manuals we reviewed except for the USAF's Monthly Acquisition Report (MAR).
- **Access, security, and dissemination**. Access and security appear to be largely the same across program types and organizations. Access to data is largely determined by the owner of those data, and rules about granting access to users are designed into the information systems hosting the data. Information security policy is set predominantly by the chief information officer (CIO), chief management officer (CMO), or chief data officer (CDO) of an organization; these policies are reflected in certification procedures and data access and dissemination rules.
- **Quality and completeness**. Data quality—accuracy, validity—is not explicitly dealt with in policy or data management practice, but data quality could be addressed during the approval processes within the Services. Completeness, in contrast, is explicitly addressed in data management policy and practices across ACAT levels and organizations. Completeness in this context means whether required data were submitted on time.

Table 1. Comparison of Framework Attributes for ACAT II–IV Acquisition Programs

(DoD, 2007)

<table>
<tr><th>Attributes</th><th>OSD</th><th>USAF</th><th>Army</th><th>Navy</th></tr>
<tr><td rowspan="3">Information governance</td><td>• Responsible for
DoDD 5000.01[a] and DoDI 5000.02 policies (overall acquisition and statutory/regulatory information requirements)</td><td colspan="3">• Aligned to OSD</td></tr>
<tr><td>• ACAT I acquisition process and information requirements clearly defined</td><td colspan="3">• Aligned to OSD</td></tr>
<tr><td>• Minimal ACAT II–III discussion except defines all ACAT levels and statutory and regulatory information requirements
• ACAT IV level not defined</td><td>• USAF ACAT II–III information governance similar to ACAT I governance
• Detailed USAF ACAT I–III acquisition information framework defined in policy</td><td>• Limited Army ACAT II–IV information framework</td><td>• Navy ACAT II–IV information
governance similar to ACAT I governance
• Detailed Navy ACAT I–IV acquisition information framework defined in policy</td></tr>
<tr><td rowspan="4">Roles, responsibilities, and authorities</td><td colspan="4">• Generally specified in policy for ACAT I–IV programs (except OSD does not define ACAT IV programs)</td></tr>
<tr><td>• Limited responsibilities for program information collection, storage, and dissemination</td><td colspan="3">• Limited and decentralized responsibilities for program information collection, storage, and dissemination</td></tr>
<tr><td rowspan="2">• One main office responsible for management of various ACAT I program information</td><td>• Air Force Acquisition Executive organization dedicated to managing ACAT I–III data</td><td>• Army PEOs and PMs are entirely responsible for managing
ACAT I–IV data</td><td>• Navy Acquisition Executive organization dedicated to managing ACAT I–IV data
• Position includes governance and management</td></tr>
<tr><td colspan="3">• PMs generate or collect the majority of program information</td></tr>
<tr><td>Use cases</td><td colspan="4">• Use cases for acquisition program data are largely similar across OSD and the Services and across ACAT levels</td></tr>
</table>

Table 1. Comparison of Framework Attributes for ACAT II–IV Acquisition Programs (Continued)

Attributes	OSD	USAF	Army	Navy
Processes	• Milestone, event-driven acquisition process well defined in OSD policy	• Milestone, event-driven acquisition process well defined in USAF policy	• Milestone, event-driven acquisition process well defined in Army policy for ACAT I programs but less defined for ACAT II–IV programs	• Milestone, event-driven acquisition process well defined in Navy policy
	• Process both generates program data through program execution and consumes program data in milestone decisions and technical reviews			
Authoritative data and definitions	• Authoritative data fields defined in DAMIR/DAVE information systems for ACAT I programs	• Authoritative data fields defined in USAF PMRT information system for ACAT I–III programs	• Army uses OSD’s authoritative data fields and definitions for ACAT I information • Has authoritative source for limited ACAT II–IV	• Authoritative data fields defined in Navy RDAIS information system for ACAT I–IV programs
	• Core data elements appear largely the same (e.g., cost, schedule, performance) but are presented differently across OSD and Services			
	• Specific data elements and metrics tailored to organization’s culture, historical precedents, and preferences of the current senior leadership			
Data, business, and system rules	• At the ACAT I level, OSD has worked with USAF and the Navy to electronically align collection and transmission of OSD-required data		• Army uses OSD data, business, and system rules because it manually inputs ACAT I information	• ACAT I electronically aligned with OSD (see first comparison to the left)
	• Does not manage business rules for ACAT II–IV programs; documented some for ACAT I programs	• Business rules for ACAT II–III program information are documented for MAR	• Army uses OSD information system for limited ACAT II–IV information	• Business rules for ACAT II–IV program information are minimally documented

Table 1. Comparison of Framework Attributes for ACAT II–IV Acquisition Programs (Continued)

Attributes	OSD	USAF	Army	Navy
Access, security, and dissemination	• Access and security appear largely the same across program types and organizations		• Army does not have an information system for program information, uses OSD's security for ACAT I information • The AAPML user guide describes how Army secures, provides access, and disseminates its limited ACAT II–IV information	• Aligned with OSD and USAF comparison to the left
	• Access to data determined by owner of that data (often the originator of the data; e.g., a program office)			
	• A user's account is granted permissions for inputting, viewing, and using data appropriate to user's role in the acquisition process			
	• Information security policy is set predominantly by CIO, CMO, or CDO of an organization			
Quality and completeness	• Data quality—accuracy, validity—not explicitly addressed in policy or data management practice			
	• Completeness explicitly addressed in data management practices across ACAT levels and organizations; typically refers to whether required data was submitted			

Alignment of OSD and Service data policy and management environments creates efficiencies and potential savings with respect to program data collection, storage, processing, and sharing. Adopting common definitions on acquisition program data enables the Services to interact more seamlessly with OSD data systems; they can still tailor their own Service-specific data systems, metrics, analyses, and visualizations to satisfy the preferences of senior leaders and Service-specific use cases.

Achieving a common data framework across both program types and all organizations is a complex task. It requires some degree of alignment of attributes of both the policy and data environment. At a minimum, there needs to be agreement on a core set of data to be recorded (defined in policy) and the definitions of associated data elements and data fields; information governance organizations and processes need to be established and aligned to manage and oversee data-related activities. Use cases defined in policy and practice do not need to align precisely, but the underlying data required by those use cases do. Technical parameters of the information systems also do not need to align perfectly, as long as it is possible to transfer data between them without introducing errors.

A major challenge in achieving a common data framework is overcoming cultural barriers that often prevent data-sharing and transparency. ACAT I programs have a common framework, but this framework is only partially reflected in current law, regulations, policy, and guidance. Services coordinate with the OSD in different ways for ACAT I programs; for ACAT II–IV, Services largely use the ACAT I data framework (data definitions), share program lists, and use the OSD APB module but do not share cost, schedule, and performance information with the OSD. Semantics (definitions, data elements, and business rules) for smaller programs are reflected in Service policies or user guides to varying degrees. In all cases, the Services are actively improving their data governance and management practices for both internal use and coordination with the OSD.

Options to Consider for Improving the Current DoD Program Data Environment

Acquisition program data managers in the DoD appear to agree that movement toward a common data framework or environment in some form would be beneficial across the entire DoD enterprise. More importantly, the Under Secretary of Defense for Acquisition and Sustainment and other DoD leadership cannot have insight into their missions without these data. Examples of potential benefits are improved communication, data-sharing, leveraging of existing data systems (as opposed to developing, operating, and maintaining Service- or program-unique data systems), improved transparency, and improved data quality. Standardization and consistency within a common data framework could also improve analysis and program decision-making by enhancing analysis and facilitating a shared understanding of how to interpret results.

The intent of data management is to improve program management by providing higher-quality, consistent information to inform a variety of acquisition use cases. Data management emphasizes data standards—which can be common across organizations and program types—not just status reporting. We have identified five actions that we believe will facilitate continued progress toward a common environment for acquisition program data and improve acquisition data management in the DoD. Some recommendations are improvements or actions that reinforce recent trends while other recommendations are new (e.g., an enterprise acquisition data strategy).

Implementation of the options presented here will require some additional focus because the current acquisition environment is in the midst of significant change from multiple congressional mandates. Some implementation concerns are a workforce that tends to focus on process rather than data (both a cultural and training issue); the recent changes to the acquisition organizational structure within the OSD; and changes in RRA through the delegation of the majority of MDA to the SAEs.[1]

Continue the AVSG/AVWG to Facilitate Information Governance

The AVSG and AVWG structures provide an important forum for information governance. The AVSG convenes senior leaders from the OSD and the Services whose offices are directly responsible for acquisition program information, and it can be a useful mechanism for aligning policies. The AVWG, which pulls together information managers who are responsible for establishing data management practices, facilitates communication and collaboration and pro- vides a mechanism for aligning data management practices across organizations and program types. We recommend continuing the AVSG/AVWG as an important element of information governance. The recent reorganization of the OSD acquisition organizations and the rebalancing of MDA toward the Services offers an opportunity to make information governance through the AVSG/AVWG structure formal and explicit. Membership and participation can be adjusted to reflect both the new organizations and new acquisition authorities.

Promulgate an Acquisition Data Strategy for the DoD

Currently, no enterprise-wide strategy exists for acquisition program data.[2] Such a strategy— developed collaboratively with the Office of the Under Secretary of Defense for Acquisition and Sustainment, the Office of the Under Secretary of Defense for Research and Engineering, and the SAEs—could set the parameters of a common data framework and environment. It could also encourage sharing of ideas and experiences, improve data transparency and access, and establish goals for a common data framework. An enterprise acquisition program data strategy could become a significant element of acquisition information governance. The DoD might want to consider addressing the need for core definitions in this strategy, along with considering communication mechanisms and other best practices in information management.

Focus Initial Efforts on Identifying a Core Set of Acquisition Program Data

Small steps and incremental change are often easier and more effective than trying to do everything at once. We therefore suggest developing an initial common data framework based on a small set of core program data appropriate for all program types and use cases. (This is in addition to the APL that has been recently added to DAVE.) At first, these data might be just program descriptive information; additional data elements could be

[1] Section 825 of the National Defense Authorization Act (NDAA) for Fiscal Year 2016 (as amended) states that the milestone decision authority [MDA] for a major defense acquisition program reaching Milestone [MS] A after October 1, 2016, shall be the service acquisition executive of the military department that is managing the program, unless the Secretary of Defense [SECDEF] designates … another official to serve as the milestone decision authority.

See also 10 U.S.C. §2430[d]. Section 901 of the NDAA for Fiscal Year 2017 instituted a major reorganization within the OSD and created three new positions: Under Secretary of Defense for Research and Engineering, Under Secretary of Defense for Acquisition and Sustainment, and a CMO.

[2] The USAF CDO is working toward a Data Architecture Charter and Data Services Reference Architecture for “all” USAF data (including acquisition data) and has set a vision to foster a data-driven organization by enabling Air Force activities through Visible, Accessible, Understood, Linked, and Trusted data.

added incrementally. The focus should fall on the underlying data, not the specific metrics preferred by a particular senior leader. This recommendation builds on the success that information managers have already achieved through both formal (i.e., AVWG) and informal mechanisms, and following through on this action would build positive momentum toward a common data framework by enabling the institutionalization of small successes. For example, the common data definitions already in place for ACAT I programs would provide a good starting point because they are already defined and do not create additional burden to collect. In addition, the Air Force and Navy have already extended some of those definitions to lower ACAT-level reporting.

Leverage Existing Program Data Infrastructure

In this context, *infrastructure* means established information systems and applications running on those systems as well as approved and agreed-upon definitions for data elements and data fields. There is no reason to invest in all new Service- or application-specific information systems when existing systems can be expanded or otherwise modified to accomplish the same end.

Establish a Common Definition of a Program and Program Start

Acquisition program data collection begins with the definition of a program.[3] Until an activity is officially declared a program, many of the information requirements do not apply. These activities can be for weapons, business systems, and Middle Tier efforts, to name a few. The high variation in the number of ACAT III programs counted among the Services suggests that the definition of a program might differ. DoDI 5000.02 (DoD, 2017) currently defines program start at MS B for ACAT I programs; policy is unclear as to when ACAT II–IV programs officially start.

This lack of clarity raises several questions that need to be answered:

- Who is the authoritative source for identifying when an activity becomes a program?
- When is a given set of activities both related enough and mature enough to declare it a program?
- What information should be documented and reported about a program early in its life cycle?

We recommend that the DoD develop a single definition of a program. The definition should include criteria and procedures for declaring program start, as well as a determination of the minimum program data needed at program start. A small set of program descriptive information can usefully be documented and applied across program type and size. This information should include program name, a unique identifier, mission or capability description, and basic cost and schedule estimates (recognizing the uncertainty of the last two data elements).

[3] The Air Force, the Navy, and the Army have provided the OSD with APLs that are now stored in the OSD's DAVE for ACAT I–IV programs. Although there is still not agreement across the DoD on the definition of a program, this nevertheless reflects progress since 2015, when the DoD could not provide the GAO with a list of non-major programs.

This study has documented the current policy and data environment for acquisition programs. Given the large shift in organizational RRA within DoD acquisition over the past few years, now would be the ideal time for the DoD to take additional strides in improving how it manages its acquisition information and consider a common data framework for its acquisition programs by its data governance function.

References

DoD. (2007, November 20). *The defense acquisition system* (DoD Directive 5000.01). Washington, DC: Author.

DoD. (2017, August 10). *Operation of the defense acquisition system* (DoD Instruction 5000.02, incorporating change 3). Washington, DC: Author.

GAO. (2015, March). *Defense acquisitions: Better approach needed to account for number, cost, and performance of non-major programs* (GAO-15-188). Washington, DC: Author. Retrieved from https://www.gao.gov/assets/670/668783.pdf

McKernan, M., Moore, N. Y., Connor, K., Chenoweth, M. E., Drezner, J. A., Dryden, J., … Szafran, A. (2017). *Issues with access to acquisition data and information in the Department of Defense: Doing data right in weapon system acquisition* (RR-1534-OSD). Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR1534.html

McKernan, M., Riposo, J., Drezner, J. A., McGovern, G., Shontz, D., & Grammich, C. (2016). *Issues with access to acquisition data and information in the Department of Defense: A closer look at the origins and implementation of controlled unclassified information labels and security policy* (RR-1476-OSD). Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR1476.html

McKernan, M., Riposo, J., McGovern, G., Shontz, D., & Ahtchi, B. (2018). *Issues with access to acquisition data and information in the Department of Defense: Considerations for implementing the Controlled Unclassified Information Reform Program* (RR-2221-OSD). Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR2221.html

National Defense Authorization Act for Fiscal Year 2016, Public L. No. 114-92 (2015).

National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328 (2016).

Riposo, J., McKernan, M., Drezner, J. A., McGovern, G., Tremblay, D., Kumar, J., & Sollinger, J. (2015). *Issues with access to acquisition data and information in the Department of Defense: Policy and practice* (RR-880-OSD). Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR880.html

Evaluating the Use of Public Data Sources to Improve Acquisition Processes: A Market Research Use Case

Dorcas L. Lasalle—Principal Investigator and Lead Acquisition and Program Management Analyst at The MITRE Corporation, supports a variety of sponsors with full acquisition life cycle support services. She has more than 15 years of experience in acquisition and contracting, both federal government and industry. She is a former Veterans Affairs and Government Accountability Office contract specialist and former Acquisition Specialist with the Department of Defense Office of Inspector General. She holds a BS in Hospitality Management from the University of Central Florida. She was FAC-C Level certified in Contracting while in civil service. [dlasalle@mitre.org]

Kristin Fitzgerald—is a Senior Data Scientist in the Model-Based Analytics Department within MITRE. She is passionate about finding ways to apply machine learning and data analytics to a variety of public service applications, including veterans' benefits, child welfare, the opioid epidemic, and the federal acquisitions process. She earned a BSE in Operations Research and Financial Engineering from Princeton University and is currently completing an MS in Analytics through the Georgia Institute of Technology. [kafitzgerald@mitre.org]

Abstract

This research describes how a FAR Part 10 market research report can be generated by integrating acquisition data from multiple government-maintained public databases into a single portal. This effort builds upon the wealth of federal acquisition data made public through several initiatives to increase government transparency and data sharing, including the DATA act of 2014. The overall study aims to demonstrate how inefficiencies in the acquisition process can be addressed through tailored design of data-driven decision support tools.

Introduction and Motivation

Acquisition processes are time and resource intensive and rely heavily on staff experience and expertise. Unfortunately, this expertise can be hard to find. In particular, the process for creation of market research reports is not standardized; they are typically compiled manually by relatively inexperienced staff who may not have the time or knowledge to integrate relevant data from different sources. As a result, given the overall acquisition strategy and execution rely heavily on elements of this market research, there is potential for significant downstream decision-making inconsistencies and delays.

Over the past few years, however, the federal government has made a large amount of acquisition data publicly available. The data is predominantly historical in nature and presents an opportunity to help develop automated decision support tools, in this instance supporting market research. Unfortunately, these datasets are of varying size and scope and are typically siloed. Even when valuable and relevant datasets are identified, they may be difficult to access or the relationships between them are not immediately clear. Greater research efforts are required to better understand the overall landscape of this data and its potential for practical use.

This research addresses a preliminary first use case application of public data sought to aid the development of a FAR Part 10 market research report by integrating acquisition data from multiple government-maintained public databases into a single portal.

Background and Past Research

A literature review to understand the current applications of data analytics and use cases for data-driven acquisition decision making determined that

a. The use of predictive analytics is being studied within government agencies as well as academia and private industry:

   - Dai and Li (2016) discussed the development of applications for non-government "armchair auditors" to analyze acquisitions data; as data is not in a consistent format, analysis is difficult without a standardized application. Applications included data reliability, suspicious supplier detection, abnormal pricing, and abnormal bidding.

b. Research has focused on using analytics to improve the following acquisitions functions:

   - *Cost estimations/budget overruns*: Adoko, Mazzuchi, and Sarkani (2015) proposed a predictive model that analyzes the impact of system performance, Technology Readiness Level (TRL), schedule, risk, and reliability on the Nunn-McCurdy significant cost overrun guidelines. Tracy and White (2011) generated models to estimate the cost of completion of contracts at varying stages of completion. Morgan (2013) uses data analytics to evaluate the use of performance-based contracts as a cost-saving measure. Reed, Keller, and Fallon (2016) review cost per dollar obligated measurement in defense contracts and show the use of analytics to show trends beyond dollars spent.
   - *Requirements development:* Dargan et al. (2014) developed a statistical model of the relationship between requirements quality and operational results, using data from the DoD and DHS.
   - *Performance:* Knudsen and Blackburn (2016) propose a predictive model to examine project schedule performance. Apte, Rendon, and Dixon (2016) explored how the DoD can leverage acquisition data, specifically contractor performance information, in identifying drivers of success in services acquisition using big data techniques. Guillaume-Joseph and Wasek (2015) used historical aspects of software project failure to develop a predictive model that can be used in acquisitions.
   - *Regulation:* Patrignani (2014) evaluated the impact of changes to the FAR in 2009 on contractor misconduct focusing on the impact of penalties for misconduct using statistical analysis. Tkach (2017) examined USSOCOM's acquisition and procurement processes, policies, and challenges and provides insight into nontraditional DoD contracting by studying historical data.

c. A variety of analytical methods are being used:

   - *Natural Language Processing (NLP)/text mining:* Gao, Singh, and Mehra (2012) developed a tool (Contract Miner) to extract data from service contracts using NLP. Yang et al. (2013) developed a prototype NLP tool to analyze contract service agreements (CSAs). Chalkidis, Androutsopoulos, and Michos (2017) studied how legal contract element extraction can be automated using NLP and machine learning.

- *Predictive regression:* Miller (2012) examines the use of text mining in acquisitions management and combines that with predictive regression models to determine cost estimate changes.
- *Bayesian/statistical modeling:* Knudsen and Blackburn (2016) used a Bayesian model to predict schedule performance.
- *Agent-based simulation:* Schwenn et al. (2015) introduced a research methodology for examining the U.S. weapon procurement system as a complex adaptive system (CAS) and using agent-based modeling (ABM) to identify significant causal factors that contribute to the performance of the procurement system.

While the research indicated that federal acquisitions data can be analyzed to improve performance, there was limited evidence of its use at an agency- or government-wide level.

Data Sources and Integration

Phase one of the project involved collecting data from a variety of public sources, identifying relationships between the sources, and completing any required data cleaning and integration. The team collected over 20 GB of data dating back to 2013 from the following public acquisition data sources:

a. USA Spending—Contract spending records for the U.S. government, 2013–2017;

b. System for Awards Management (SAM)—List of all contractors eligible to contract with the federal government and an exclusions list of contractors excluded from contracting with the government;

c. Federal Awardee Performance and Integrity Information System (FAPIIS)—Contractors' performance and integrity records;

d. Federal Procurement Data System–Next Generation (FPDS-NG)—Government-wide procurement and spending database;

e. FBO.gov—General portal of entry for competitive acquisitions and corresponding documentation to include requirements; and

f. Interagency Contract Directory—Procurement and spending between U.S. government agencies.

As shown in Figure 1, we identified existing relationships between the sources as well as primary keys between the datasets that allowed them to be linked. In most cases, the linking key was the Dun & Bradstreet (DUNS) contractor number and/or the contract number. The Interagency Contract Directory was not used in the final Market Research prototype, so it is excluded in the figure.

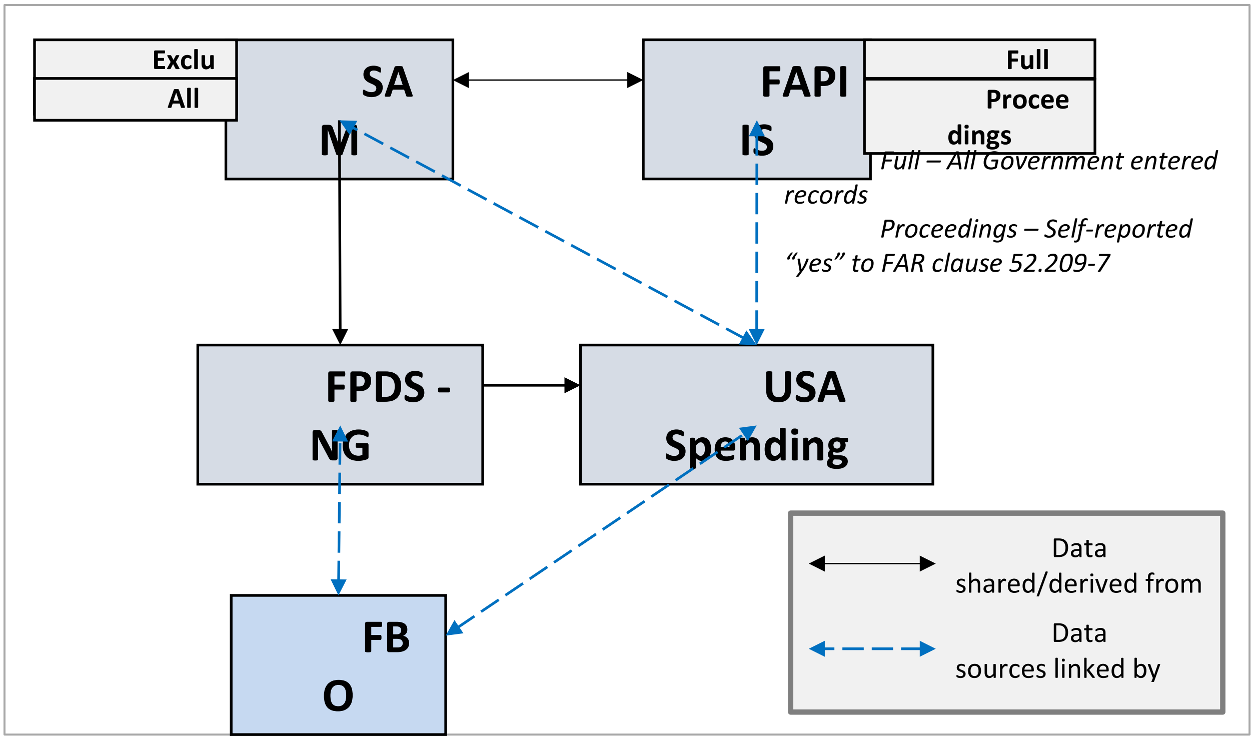


Figure 1. **Data Source Map**

Significant data cleaning was required, including the removal of duplicate records, type coercion, correction of data quality issues, and removal of nonsense characters. Data was stored using a combination of PostgreSQL and MongoDB databases.

Market Research Portal Overview

Phase two of the project consisted of developing the Market Research Portal prototype, a use case that demonstrated the data integration capabilities of the data warehouse. The team used standard agile development practices and leveraged both subject matter experts and user interactions to perform usability studies and evaluate features.

The Market Research Portal provides a market research report template as well as a system that supports an approvals process, review of older reports, and tailored instruction or template modifications by a supervisor. The key improvement of this portal over existing technology is that it automatically brings in data from the sources described previously. Based on the desired acquisition category (as defined by NAICS and/or PSC code), the portal filters to relevant vendors registered to do business with the government and provides contract history. The portal assists the user in identifying potential contractors who may or are already providing supplies and services to the government for similar requirements with additional refinement parameters such as dates and dollar amount. The portal also allows the user to search for similar requirements from other agencies and develop their own initial requirements validated by research. Lastly, the portal allows email correspondence with industry. The team applied agile development practices to update the application using feedback received from sponsors and user groups. All features were designed to meet minimum report requirements based on widely used agency templates and user feedback sessions.

A diagram of the project technical architecture is included in the appendix.

Walkthrough of Prototype Features

The set of features described next was created based on a series of user stories developed by subject matter experts, which were then adjusted or supplemented by user testing and feedback.

1. **Login and Report Overview:** The system is protected by a user login and password; this can be tailored to a specific government agency or to use a CAC card. Once logged in, a user encounters a list of generated reports. The user has an option of creating a new report, editing an existing report, sharing a report (e.g., for approval), exporting a report, or deleting a report.
2. **Report Creation:** When a user creates a new report, they give the report a title and limit the scope of the report using a NAICS and/or PSC code. These codes are later used for database search and aggregation. The user supplies a narrative description of services and other relevant background information. They also provide specifications of supplies/services as well as a list of requirements. Additionally, they specify the period of performance.
3. **Vendor:** The user is then able to explore the set of potential vendors. This vendor list is already filtered based on the NAICS/PSC information initially provided. The user may search the vendors for specific keywords and may also filter the vendors by whether they have been awarded contracts previously, by various small business categories, by the dollar value of past contracts, and by whether they have performance or integrity issues recorded (based on FAPIIS records and SAM exclusions).

   For each vendor, the user has the opportunity to examine information about prior contracts and select vendors they are interested in researching further.
4. **Research:** For each vendor selected, the user may enter notes, assign requirements to the vendor, and view vendor contact information. The portal also gives the user the option to send a standardized email to each vendor asking for answers to questions and to get quotes. The research phase also allows the user to search FBO for similar requirements by NAICS or description and also provides a list of Government-Wide Acquisition Contracts (GWACs) that meet the requirements.
5. **Analysis:** In analysis, the information from all the previous phases are merged together into a single summary that the user can annotate and view. The analysis section has the greatest room for growth based on individual organizations' needs (discussed below).
6. **Recommendations:** Finally, the user can summarize their findings into a recommendation, which may include details such as contract type, contract vehicle type, solicitation strategy, key differentiators for source selection, and the identification of strong candidate contractors. The report can then be exported to a pdf, saved for later, or sent for approval to others.

Additional potential features are discussed in our conclusions.

User Testing and Review

Initial user testing leveraged MITRE subject matter experts who had extensive experience in creating market research reports as previous federal employees or contracted support staff. We also received feedback from several sponsors during the design and build process. Consistently, we were told that a tool like this would reduce the time required to complete the highly manual portion of the market research process (finding, accessing, extracting the data from many sources, then aggregate and execute reviews of information) and would enable users to dedicate more time into their thought-driven analysis and benchmarking of strategy and approach to the acquisition. Many of the features discussed previously were derived through user testing and interviews, including the ability to contact potential vendors through the tool. Test users also helped to identify which contract information was most relevant for their analysis, and which vendor characteristics they would like to be able to use as a filter. One feature that was highlighted frequently as important and increasingly relevant was the ability to determine a contractor's small business status and to compare that vendor's contract history with other vendors.

In the future, we will quantify the value added by this tool by running a controlled experiment. In the experiment, several users will be asked to create a market research report using either a simple template (that is similarly formatted to the portal report) or using the designed prototype leveraging all the data sources. Users will be asked to (a) report time required to complete the report and (b) describe how well they believe they were able to complete each report and their experience building the report.

Conclusions and Recommendations

It is evident that leveraging historical acquisition data can play a part in expediting administrative acquisition functions, in this case as part of the fully standardized market research report, which can then inform decisions. The realm of decisions aligned to the data sources selected in this research addresses estimates, contractor responsibility, integrity and performance, alternatives for contract type, contract vehicle type, and meeting small business goals. The generated report is another stepping stone towards standardizing the onset of educated consumerism (market expertise) in the public sector. The prototype is designed to demonstrate the viability of such a tool when it leverages these types of data sets. An assessment of technologies and sources should be made when making a business case for such a tool on a case by case basis for each agency. The MITRE Corporation–developed prototype demonstrates the value added by integration of public acquisition data sources into a single, easy-to-use system. Since MITRE is a manager of the Federally-Funded Research and Development Center, this prototype design and utilization is available to the public sector for its application completely free of charge. Transfer of the prototype will identify frameworks, templates, and processes needed to adopt the construct for federal agency use.

Ongoing research will include going beyond the data synthesization and into how artificial intelligence and predictive analytics may be applied to better customize acquisition decision-making.

References

Adoko, M. T., Mazzuchi, T. A., & Sarkani, S. (2015). Developing a cost overrun predictive model for complex systems development projects. *Project Management Journal*, *46*(6), 111–125.

Apte, U., Rendon, R., & Dixon, M. (2016). *Big data analysis of contractor performance information for services acquisition in DoD: A proof of concept*. Monterey, CA: Naval Postgraduate School.

Chalkidis, I., Androutsopoulos, I., & Michos, A. (2017). Extracting contract elements. In *Proceedings of the 16th International Conference on Artificial Intelligence and Law* (pp. 19–28).

Dai, J., & Li, Q. (2016). Designing audit apps for armchair auditors to analyze government procurement contracts. *Journal of Emerging Technologies in Accounting*, *13*(2), 71–88.

Dargan, J. L., Campos-Nanez, E., Fomin, P., & Wasek, J. (2014). Predicting systems performance through requirements quality attributes model. *Procedia Computer Science*, *28*, 347–353.

Gao, X., Singh, M. P., & Mehra, P. (2012). Mining business contracts for service exceptions. *IEEE Transactions on Services Computing*, *5*(3), 333–344.

Guillaume-Joseph, G., & Wasek, J. S. (2015). Improving software project outcomes through predictive analytics, part 2. *IEEE Engineering Management Review, 43*(3), 39–49.

Knudsen, K. T., & Blackburn, M. (2016). A knowledge and analytics-based framework and model for forecasting program schedule performance. *Procedia Computer Science*, *95*, 319–326.

Miller, T. (2012). *Acquisition program problem detection using text mining methods*. Wright-Patterson Air Force Base, OH: Air Force Institute of Technology.

Morgan, C. (2013, Summer). Best practices of developing performance-based acquisitions to save the U.S. federal government money. *Journal of Contract Management,* 77–86.

Patrignani, J. O. (2014). *Impact of federal acquisition regulation change on contractor misconduct*. Minneapolis, MN: Walden University.

Reed, T., Keller, J., & Fallon, J. (2016). *Organization analytics: Taking cost-per-dollar-obligated (CPDO) measures to the next level in defense contracting* (No. SYM-AM-16-068). McLean, VA: Beyond Optimal Strategic Solutions.

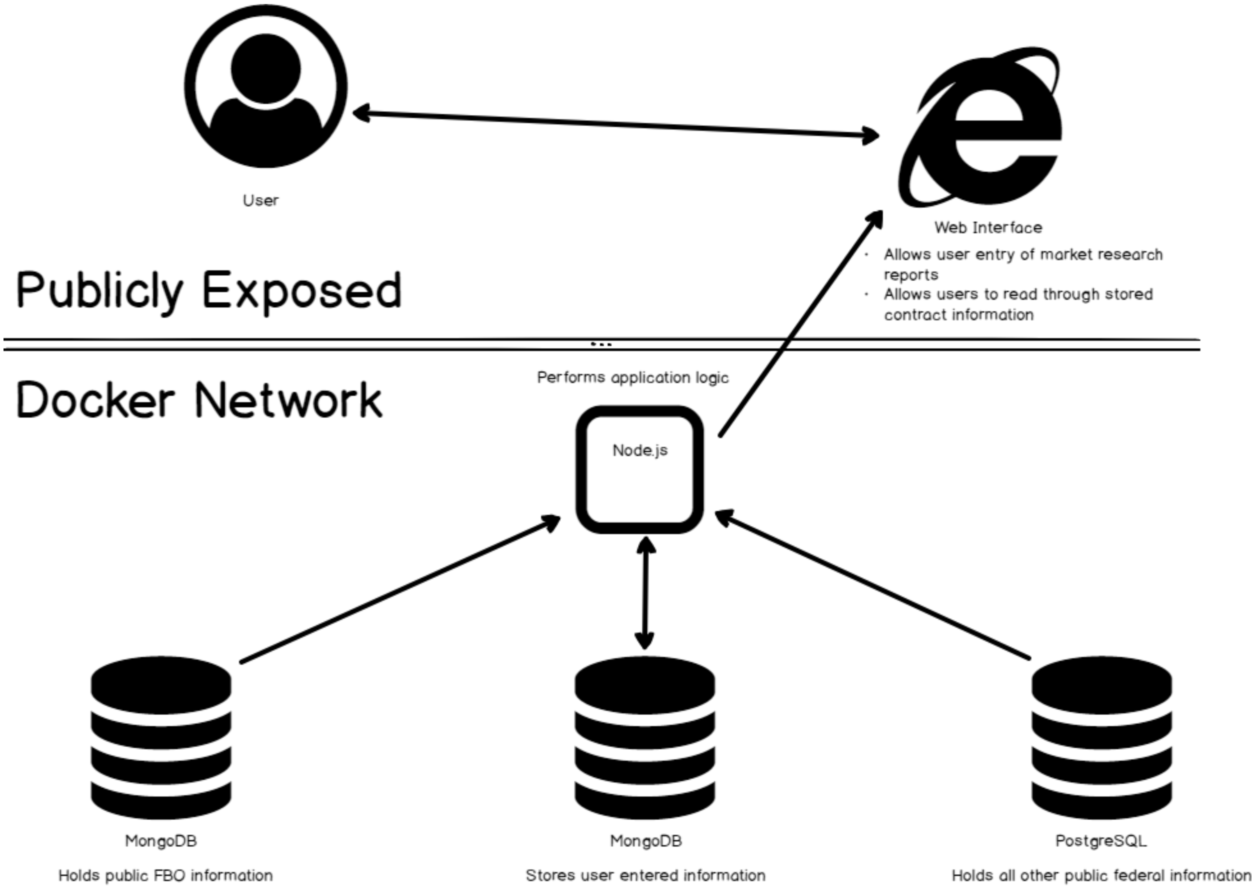
Schwenn, K., Colombi, J., Wu, T., Oyama, K., & Johnson, A. (2015). Toward agent-based modeling of the U.S. Department of Defense acquisition system. *Procedia Computer Science*, *44*, 383–392.

Tkach, B. (2017). *Special operations contracting: 21st century approaches for service and technology acquisition* (Joint Special Operations University Report 17-5).

Tracy, S. P., & White, E. D. (2011). Estimating the final cost of a DoD acquisition contract. *Journal of Public Procurement, 11*(2), 190–205.

Yang, D. et al. (2013). A natural language processing and semantic-based system for contract analysis. In *Proceedings of the 2013 IEEE 25th International Conference on Tools with Artificial Intelligence* (pp. 707–712).

Appendix. Market Research Portal Architecture


User
Web Interface
Allows user entry of market research reports
Allows users to read through stored contract information
Publicly Exposed
Docker Network
Performs application logic
Node.js
MongoDB
Holds public FBO information
MongoDB
Stores user entered information
PostgreSQL
Holds all other public federal information

Acquisition Research Program
Graduate School of Business & Public Policy
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net