Interim Report and Third Quarter Recommendations

October 2020

NATIONAL
SECURITY
COMMISSION
ON ARTIFICIAL
INTELLIGENCE

Commissioners

DR. ERIC SCHMIDT
Chairman

HON. ROBERT O. WORK
Vice Chairman

SAFRA CATZ

DR. STEVE CHIEN

HON. MIGNON CLYBURN

CHRISTOPHER DARBY

DR. KENNETH FORD

DR. JOSÉ-MARIE GRIFFITHS

DR. ERIC HORVITZ

ANDREW JASSY

GILMAN LOUIE

DR. WILLIAM MARK

DR. JASON MATHENY

HON. KATHARINA MCFARLAND

DR. ANDREW MOORE

Contents

Letter from the Commission Co-Chairs

In the past few months, the artificial intelligence (AI) revolution playing out before our eyes has shaken the strategic terrain beneath our feet. The United States is in an AI-charged technology competition fusing national economic competitiveness, great power rivalry, and a fierce contest between authoritarianism and democracy. We are at the beginning of the beginning of this new competition. The principles we establish, the federal investments we make, the national security applications we field, the organizations we build, the partnerships we forge, and the talent we cultivate now will set America's strategic course.

The Commission wants to convey one big idea. The countries, companies, and researchers that win the AI competition—in computing, data, and talent—will be positioned to win a much larger game. AI is accelerating innovation in every scientific and engineering endeavor. The entire innovation base supporting our economy and security will leverage AI. AI is compressing innovation timescales. Once fantastical ideas in areas like biotechnology will become realities in the near future. The arc of steady AI research has become a step function in AI capabilities. Just recently, an AI-powered text generator produced paragraphs of prose as if written by a human. News about progress in brain-computer chip interfaces presages the melding of human thought and machine power. In defense, the U.S. military tested an AI-powered command and control system that shot down a cruise missile with a "smart bullet," demonstrated that an AI controlled fighter jet could defeat an experienced pilot in a simulated dogfight, and used AI to cut design costs for aircraft through modeling and simulation. Meanwhile our adversaries are not just testing. They have employed AI-generated online personas in disinformation campaigns against us.

Against this dizzying backdrop, the Commission has taken an entrepreneurial approach by necessity. This report represents our third quarterly memo as well as our second interim report mandated by Congress. Below we present 66 recommendations flowing from several key ideas. First, we must defend democracies from AI-enabled disinformation and other malign uses of AI by our adversaries. Second, the government should expand and democratize basic AI research—the wellspring of our technological advantages. Third, the government must build a digital ecosystem within national security departments and agencies for AI R&D. Fourth, connecting technologists and operators will be the key to leveraging AI in all national security missions. Fifth, we must close the tech talent deficit by strengthening STEM education, recruiting the best minds from around the world, and training the national security workforce. Sixth, we must build a resilient domestic microelectronics industrial base. Seventh, we will need interconnected strategies for technologies associated with AI including biotechnology and quantum computing. Eighth, we cannot only focus on domestic initiatives in a global competition. We must lead the development of AI technical standards and norms in international forums, and strengthen AI partnerships with allies and partners to build a digital future reflecting our values and protecting our interests.

The totality of the recommendations illustrates a key point: Laying out a vision is not enough. A winning strategy demands major muscle movements in and across departments and agencies, and significant executive and legislative action. It requires overcoming the technical, bureaucratic, and human obstacles to change, and driving very specific policies.

We believe the United States needs a new White House-led technology council to elevate AI-driven technology developments to the center of national decision-making, and a technology advisor to lead a new technology competitiveness strategy that integrates the complex interplay between technology, national security, and economic policies.

The Commission still has much work to do before delivering its final recommendations in March 2021. Looking under the hood of the vast national security enterprise yields frustration but not hopelessness. Innovators throughout our government and in the private sector and civil society are working hard. Leaders in Congress, the Executive Branch, and across the United States are eager to act. The Commission is determined to help them succeed.

Summary of Third Quarter Recommendations

Line of Effort (LOE) 1: Invest in AI Research and Development (R&D)

Progress to Date: Research remains the foundation of America's technological leadership, and the government must make the investments to solidify this foundation for artificial intelligence (AI). In the First Quarter (Q1), the Commission recommended doubling non-defense AI R&D funding, focusing investments on six priority research areas, and launching a pilot of a National AI Research Resource. In the Second Quarter (Q2), the Commission examined the Department of Defense (DoD) research enterprise and recommended ways to overcome bureaucratic and resource constraints to accelerate national security-focused AI R&D.

TAB 1 — Strengthening the Triangular Alliance for AI R&D

Focus: America's ability to harness innovation is predicated on a rich interplay between academia, government, and industry—and organizations that straddle those lines—where each sector benefits from and relies on the advances of the others. To support the level of AI research, development and application that will underpin future U.S. technological leadership, the government must take action to strengthen the alliance by exploring new mechanisms to support research and enable partnerships with industry.

Objective: In order to strengthen the triangular alliance and position the United States for an AI-enabled future, the Commission proposes actions to address three priority issue areas:
1) Supporting the growth of nationwide AI R&D through novel funding mechanisms;
2) Posturing the defense and intelligence AI R&D communities to address national-security specific problems and capabilities through establishment of a modern digital ecosystem; and
3) Expanding the role of industry in the DoD's AI R&D to pursue next-generation capabilities.

Issue 1: Supporting AI Research through Novel Funding Mechanisms

Recommendation 1: Create an AI Innovator Award Program to Invest in Top Talent. Foster high-risk, exploratory research through the launch of a program that makes long-term, high-value awards that provide top researchers the flexibility to pursue big ideas without prescribed outcomes.

Recommendation 2: Invest in Research Teams Pursuing Transformative Ideas in AI. Establish a team award that supports multi-disciplinary, bold research initiatives to apply AI to solve complex problems or pursue use-inspired basic research efforts.

Recommendation 3: Create AI Testbeds to Serve the Academic and Industry Research Communities. Develop a set of national, domain-specific AI testbeds to provide ready infrastructure, benchmarking standards, and build communities of discovery and practice around application areas for AI that are in the public interest.

Recommendation 4: Support AI Data Set Curation and Maintenance. Start a program to curate, host, maintain, and make publicly accessible complex, exemplar data sets to help drive research progress in AI and its application to other fields of study.

Recommendation 5: Launch an AI Research Challenge. Open a Defense Advanced Research Projects Agency (DARPA) Grand Challenge around an ambitious AI-enabled goal that would focus on accelerating progress on third wave AI capabilities and advancing technology that could plausibly drive future defense capabilities, such as human-robotics teaming and human-AI collaboration.

Issue 2: Creating a Digital Ecosystem for National Security AI R&D

It is necessary to equip researchers and developers within the national security community with the services, tools, and environments necessary to accelerate innovation in AI. This should be accomplished through a networked architecture supporting a diversity of AI approaches that connects researchers and developers to federated repositories hosting data, trained AI models, and AI software tools made accessible through user-based authentication; along with AI testbeds and test ranges; and distributed computing resources and support. *NOTE: Implementation recommendations will be developed for inclusion in the final report.*

Issue 3: Expanding Industry's Role in DoD's AI R&D to Develop Next-Generation Capabilities

Recommendation 6: Communicate DoD Modernization Priorities to Industry through Issuance of Technology R&D Objectives. Publish R&D objectives through the Office of the Undersecretary of Defense for Research and Engineering (OUSD(R&E)) to support existing modernization priority roadmaps and the Technology Annex to the *National Defense Strategy*. The R&D objectives should be tied to subsets or components of the modernization priorities on which the government envisions the private sector playing a major role in building future capabilities.

Recommendation 7: Strengthen Return on Small Business Innovation Research (SBIR) Investments. Optimize the DoD's SBIR program to more effectively develop and deploy AI solutions to meet warfighter needs. Enable successful prototypes to scale through sufficient funding, early access to customers and operators, and better due-diligence. Review, modernize, and streamline DoD SBIR process to encourage broader participation of American technology start-up and small business companies.

Recommendation 8: Launch an AI Catalyst Initiative. Overseen by a joint council composed of OUSD(R&E), the JAIC, and Service leadership and executed by DARPA or the Services' innovation entities, the AI Catalyst Initiative (AICI) would accelerate research by non-traditional contractors into longer-time-horizon, next-generation defense capabilities—supporting the evolution from basic research to easily scalable prototypes. The initiative would fund and facilitate several multi-year partnerships between operators/end-users and teams of private sector researchers driving toward a slate of research priorities.

LOE 2: Applying AI for National Security

Progress to Date: The United States must maintain global leadership in AI/ML application for U.S. national security and defense. In Q1 the Commission recommended top-down leadership mechanisms to strengthen existing AI initiatives and accelerate DoD AI application in the near-term by establishing a Steering Committee on Emerging Technology, tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence; elevating the Director of the Joint Artificial Intelligence Center (JAIC) to report directly to the Secretary of Defense (or Deputy Secretary of Defense); and endorsing the need for the JAIC Director to remain a three-star billet with extensive operational expertise. Q2 recommendations focused on establishing clear guidance to direct resourcing and investments in disruptive technologies via a classified technology annex linked to the operational challenges identified in the National Defense Strategy. Q2 recommendations also proposed actions to incorporate AI/ML into concept development through Joint and Service exercises; bolster experimentation efforts; and increase the Department's institutional agility through modernization of its core administrative functions.

TAB 2 — Applying Artificial Intelligence for National Security Missions

Focus: The Commission proposes options to maximize the impact of DoD's Chief Technology Officer (CTO), the Under Secretary of Defense for Research & Engineering (USD(R&E)), and to designate an Intelligence Community (IC) CTO. The seven options below are not mutually exclusive from one another and build on the recommendations made in Q1 and Q2.

Objective: To maintain advantage in a technological competition with near-peer competitors, the DoD and the IC must organize for speed and agility, integrating the perspectives of technologists and operators at every level. The options below aim to deliver this integration by driving closer coordination with the military services and intelligence entities as they conduct R&D, planning, budgeting, and acquisition activities; and providing funding mechanisms to incubate and mature promising technology that would otherwise not make it from lab to field.

Recommendation 1: USD(R&E) should integrate DoD's technology scouting community of practice, leveraging AI-enabled analytics to provide authoritative technology inputs for national security planning. Assign USD(R&E) as the Executive Agent responsible for producing the *National Defense Strategy* Technology Annex, convening a technology scouting community of practice to collaborate in development of the Annex. Reestablish the Strategic Intelligence Analysis Cell (SIAC) Director as a direct report to the USD(R&E). Increase SIAC funding for expanded investments in AI tools, commercial data, and a diverse technology fellows program.

Recommendation 2: USD(R&E) should be appointed the Co-Chair and Chief Science Advisor to the Joint Requirements Oversight Council (JROC) for Joint and cross-domain capabilities. To accelerate application of AI and other emerging technologies for competitive advantage, USD(R&E) must play a central role in connecting technological advancements in research and development to joint operational requirements.

Recommendation 3: USD(R&E) should have a dedicated fund to mature, operationally prototype, and transition exceptionally promising AI-enabled technologies. DoD's budget process poses a significant obstacle to transitioning advances in the lab to capabilities in the field. In the current budget system, and given today's rate of technological change, program managers will increasingly struggle to rapidly identify, fund, and incorporate promising technologies into their programs. Without available program funds at the end of a defense science and technology (S&T) project's life cycle, the technology can stall or be abandoned before it can be evaluated in a realistic environment and a determination made as to the capability improvement it could deliver. To move as fast as U.S. competitors and maintain the defense advantage, DoD must have a means to support promising AI projects beyond early-stage research and development even when planned program funding is not yet in place.

Recommendation 4: Within the Office of the Director of National Intelligence (ODNI), the Director of S&T should be designated as the IC's CTO and empowered to enable the IC to adopt AI-enabled applications to solve operational intelligence requirements. To ensure top-down prioritization of emerging technologies and provide leadership the resources and authorities to support tech development, the Director of S&T should be designated as the IC CTO and granted additional authorities for establishing policies on, and supervising, IC research and engineering, technology development, technology transition, appropriate prototyping activities, experimentation, and developmental testing activities. Additionally, the Director of S&T should have a fund that would allow the ODNI to identify and invest in AI applications with outsized potential that may not have an identified source of agency or program funding as they near the end of their S&T life cycle.

Recommendation 5: The IC CTO, in coordination with USD(R&E), should develop a technology annex to the National Intelligence Strategy that establishes technology roadmaps to adopt AI-enabled applications to solve operational intelligence requirements. This annex would mirror the Office of the Secretary of Defense technology annex developed by USD R&E. It should identify emerging technologies and applications that are critical to enabling specific capabilities to address the IC's most pressing intelligence requirements. The main objective of the annex should be to chart a clear course for identifying, developing, fielding, and sustaining those critical emerging and enabling technologies, and to speed their transition into operational capability.

Recommendation 6: The IC CTO should establish common technical standards and policies necessary to rapidly scale AI-enabled applications across the IC and have the authority to enforce them across the IC. For the IC to integrate AI-enabled applications into its operations, it must first establish common technical standards and policies. ODNI should establish these standards and policies in close coordination with industry, adopting those standards and practices that have emerged as best practices and industry standards.

Recommendation 7: The IC should develop a coordinated and federated approach to applying AI-enabled applications to open source intelligence. The explosive ubiquity of commercial networked connectivity a.k.a the internet of everything, has generated data and information that rivals government-owned intelligence gathering systems. While there will always be a need for traditional intelligence methods and classified intelligence, the IC must rethink integrating AI-enabled analysis of open source and publicly available information into all of its work streams. AI-enabled analysis of open source and publicly available information can expose patterns and trends that human analysts would not recognize, and should be used to inform all kinds of intelligence products.

LOE 3: Talent and Workforce

Progress to Date: The *2019 Interim Report* concluded that the United States Government workforce faces a major deficit in AI knowledge and technical expertise, both military and civilian. Most of the Commission's recommendations on Federal Government recruiting, hiring, and training seek to work within the current personnel system. But the Commission has also advanced more ambitious ideas in areas where the current system falls short. Q1 recommendations addressed the government's hiring process, identifying existing talent in the civilian and military ranks, improving pipelines between universities and government, and increasing public-private talent exchanges. Q2 recommendations focused on expanding the government's base of digital talent by establishing a National Reserve Digital Corps and a United States Digital Service Academy.

TAB 3 — Train and Recruit AI Talent

Part I: Recommendations to Strengthen the AI Workforce

Focus: The United States Government needs to improve the AI literacy and proficiency of its technical workforce, organizational leaders, junior leaders, policy experts, and acquisition workforce. Without these improvements, the government will remain unprepared to buy, build, and use today's digital technology. A more digitally proficient government workforce will spend taxpayer dollars more efficiently, better secure the U.S. population and critical infrastructure, accelerate bureaucratic processes, and better represent American interests during negotiations with U.S. partners, allies, and competitors.

Objective: For departments and agencies to become AI effective enterprises, they must first overcome the challenge of developing a digitally proficient workforce, including those skilled in AI and AI adjacent roles. United States defense and intelligence agencies need a workforce with expanded AI skills and expertise. Many federal employees will require more specialized training and education to buy, build, and use AI tools and AI related technology effectively and responsibly. Just as importantly, workforce development is a journey that will change as technology, missions, and organizational structures evolve. Today's workforce initiatives are helpful, but insufficient to meet the government's needs. Bolder, more aggressive actions are needed.

Issue 1: Existing Initiatives within the Military Services

Recommendation 1.1: Support the Army AI Task Force's AI and Data Science Workforce Initiative. The Commission recommends appropriators set aside $5 million of Army Operations & Maintenance (O&M) appropriations funding in Fiscal Year (FY) 2022, and $6 million in FY 2023 and subsequent years, for the U.S. Army AI Task Force's AI and data science workforce initiative to allow the U.S. Army to continue to educate its senior leaders, begin building its technical workforce, and educate a significant portion of its end users.

Recommendation 1.2: Support the Navy Community College. The Armed Services committees should sustain support for the U.S. Naval Community College (NCC). The NCC will enroll 40,000 personnel, with 100 percent of instruction online.

Recommendation 1.3: Support the Air Force Digital University. The Armed Services committees should sustain support for the U.S. Air Force Digital University. The Commission recommends House and Senate appropriators set aside $10 million in U.S. Air Force O&M funding for the U.S. Air Force Digital University in order to allow the U.S. Air Force to significantly expand the portion of its workforce with digital skills.

Recommendation 1.4: Support the Air Force Computer Language Initiative (CLI). The Commission recommends appropriators set aside $10 million in U.S. Air Force O&M funding for the CLI in order to increase the portion of the U.S. Air Force able to code in relevant software languages.

Recommendation 1.5: Support the U.S. Air Force/Massachusetts Institute of Technology (MIT) AI Accelerator. The Commission recommends appropriators set aside $15 million in Air Force R&D funding for FY 2021 in order to accelerate the U.S. Air Force's ability to adopt AI both by improving the technology it has access to and training its workforce to build and use it.

Issue 2: Managing Civilian Subject Matter Experts

Recommendation 1.6: Accelerate Existing Occupational Series Initiatives. The Office of Personnel Management (OPM) should create software development, software engineering, data science, and knowledge management occupational series. Rather than waiting for agencies to provide a formal request for a new occupational series, OPM should ask agencies to provide supporting documents and subject matter experts to study and draft a classification policy for each occupational series.

Recommendation 1.7: Create an AI Occupational Series. OPM should create an AI occupational series. Rather than waiting for agencies to provide a formal request for a new occupational series, OPM should ask agencies to provide supporting documents and subject matter experts to study and draft a classification policy for each occupational series.

Issue 3: Recruiting Civilian Subject Matter Experts

Recommendation 1.8: Enact the Science, Technology, Engineering, and Mathematics (STEM) Corps Proposal. The DoD should, with congressional authorization and appropriation, establish an office to manage and establish a STEM Corps, including a scholarship program, advisory board, private-sector partnership program, and STEM Corps member management program. Appropriators should set aside $5 million for a STEM Corps for FY 2022 and each fiscal year thereafter.

Recommendation 1.9: Endorse an AI Scholarship for Service Proposal. Once authorized by Congress, the National Science Foundation (NSF), in coordination with the OPM, should establish an AI Scholarship for Service program modeled after CyberCorps: Scholarship for Service. This should include establishing criteria for AI centers of excellence, tuition, stipends, and a service obligation.

Recommendation 1.10: Create Digital Talent Recruiting Offices. The Departments of Defense (including U.S. military services), Energy, Homeland Security, and the ODNI should create digital talent recruiting offices that monitor their agencies' need for specific types of digital talent; recruit technologists by attending conferences, career fairs, and actively recruiting on college campuses; integrate federal scholarship for service programs into agency recruiting; offer recruitment and referral bonuses; and partner with their agencies' human resource teams to use direct-hire authorities to accelerate hiring.

Recommendation 1.11: Establish a public-private talent exchange (PPTE) program at non-DoD national security agencies. The Departments State, Treasury, Commerce, Energy, Homeland Security, and the IC should establish public-private talent exchange programs.

Issue 4: Managing Military Subject Matter Experts

Recommendation 1.12: Create New Career Fields. The military services should create career fields that allow military personnel to focus on software development, career fields that allow military personnel to focus on data science, and career fields that allow military personnel to focus on artificial intelligence. Military personnel should be able to join these career fields either upon entry into the military, or by transferring into the field after serving a period in another career field, and should have options that allow personnel to either follow a path to senior leadership positions, or specialize and focus on technical skill sets.

Recommendation 1.13: Create Additional Skill Identifiers (ASIs), Additional Qualification Designators (AQDs), Additional Military Occupational Specialties (AMOSs), and Special Experience Identifiers (SEIs) for Topics Related to AI. Military services should create or purchase training for certifications and continuing education in AI mission engineering, data engineering, safety and responsible AI engineering, and AI hardware technicians.

Issue 5: Junior Leader Training and Education

Recommendation 1.14: Integrating Digital Skill Sets and Computational Thinking into Military Junior Leader Education. The military services need to integrate understanding problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making into pre-commissioning or entry-level training for junior officers and training for both junior and senior non-commissioned officers.

Recommendation 1.15: Integrating Digital Skill Sets and Computational Thinking into Civilian Junior Leader Education. Civilian national security agencies should identify the components of their workforce that need to receive training, the type of training they need to receive, and how they should receive the training needed to create enterprise AI. This should include an assessment of which positions need to understand problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making.

Issue 6: Educating Organizational Leaders

Recommendation 1.16: Integrate Emerging Technologies Material into Courses for Officers as part of Service-level Professional Military Education. The DoD should incorporate emerging technology courses for its military officers across all phases of Service-level professional military education and should build on each other as officers progress in rank. The courses should include an introduction to the latest technology, the benefits and challenges of adapting new technologies, and ethical issues surrounding the uses of emerging technologies, including the impact of biases in these technologies.

Recommendation 1.17: Require A Short Course for General and Flag Officers and Senior Executive Service (SES) Leadership Focused on Emerging Technologies. The DoD should require emerging technology short courses for general and flag officers and SES-level organizational leaders. The courses should be taught on an iterative, two year basis, should identify the latest, most relevant technologies for senior leaders, analyze how emerging technologies can impact their organization, explain the use of AI by U.S. competition in a global context, and require a level of knowledge about emerging technology to be conversant about the latest technology, trends, and limitations.

Recommendation 1.18: Create Emerging Technology Coded Billets Within the DoD. The Armed Services committees should use the FY 2022 National Defense Authorization Act (NDAA) to require the DoD to create emerging technology critical billets within the DoD that must be filled by emerging technology certified leaders. The process to become emerging tech certified would resemble the joint qualification system.

Issue 7: Creating AI Policy Experts

Recommendation 1.19: Require Short Courses for Policy Personnel with AI-Related Portfolios. The Departments of State, Defense, Commerce, Energy, Homeland Security, and ODNI should identify policy experts whose portfolios affect or will be affected by AI, then require these personnel to successfully complete short courses covering AI, its capabilities, and policy relevant topics.

Issue 8: Training Acquisition Professionals

Recommendation 1.20: Require Emerging Technology Training for Specific Acquisition Functional Areas. The Defense Acquisition University, in partnership with USD (R&E), should annually assess the AWF's emerging technology education needs. As necessary, Defense Acquisition University (DAU) should design and offer courses addressing new AWF needs.

Recommendation 1.21: Support DAU Pilot Programs Attempting to Use AI to Tailor Pedagogy and Content to Individuals. The DoD should resource ongoing DAU pilot programs intended to AI to both curate existing DoD Acquisition Workforce curriculum content as well as to tailor the delivery of that content to individual users.

Part II: Recommendations to Improve STEM Education

Focus: This set of recommendations is designed to boost American innovation in AI. The Commission's recommendations address needs at the undergraduate and postgraduate education, and reskilling/upskilling of workers once they are in the workforce.

Objective: The Commission has focused on the gaps in talent and workforce that the United States needs in order to remain a global leader in AI. The current model of STEM education in America will not meet the challenges of tomorrow. AI is becoming ubiquitous, but the United States continues to have a lack of available AI talent. As a result, the United States faces a host of serious national security challenges that are made worse as the gap between the workforce that it needs and the talent that is available continues to widen. The United States needs to increase efforts to provide a strong STEM education to all Americans in order to create a strong economy and increase the available talent, thereby increasing its ability to compete globally and improve national security.

Issue 1: Strengthening Universities as Talent Pipelines

Recommendation 2.1: National Defense Education Act II. Much like an independent task force sponsored by the Council on Foreign Relations, the Commission recommends that Congress fund 25,000 STEM undergraduate scholarships, 5,000 STEM graduate fellowships, and 500 postdoctoral positions. The Commission recommends that Congress authorize the National Science Foundation to spend $8.05 billion to fund those scholarships over a five-year period.

Recommendation 2.2: Mid-Career Faculty Fellowships. The Commission's *Interim Report* noted the trend of AI experts leaving academia for industry as a problem for cutting edge R&D research and a remedy for the keeping quality STEM teaching talent in universities is a mid-career fellowship for recently tenured faculty. The Commission recommends that Congress support the mid-career fellowship award for AI and set aside $15 million for the fellowship.

Recommendation 2.3: Support Creation of Pilot Program for Artificial Intelligence Technology and Education Improvements for Community Colleges. In order to address the growing need for a wide range of AI proficient workers, the Federal Government should invest in a new pilot program for AI upgrades for community colleges. The Commission recommends that Congress establish the Artificial Intelligence Technology and Education Improvement Program pilot program for community colleges and set aside $30 million to fund the pilot.

Recommendation 2.4: Creation of AI-Specific Government Internships. In order to increase AI knowledge and capabilities within the United States Government, the Departments of Defense and Energy as well as National Institute of Standards and Technology (NIST) should create paid AI-specific internship positions that focus on AI R&D, AI application, and other related AI topics. The Commission recommends that Congress support the creation of an AI-specific internship program for utilization across the Federal Government and set aside $2 million for the program for the creation of 340 internships.

Issue 2: Reskilling the Workforce

Recommendation 2.5: Increase Incentives for Public-Private Job Reskilling Training. The reskilling of America's workforce is essential for the United States to keep pace with the pace of technological change and The Strengthening Career and Technical Education for the 21st Century Act to begin to address this issue. The Commission recommends that Congress support the Strengthening Career and Technical Education for the 21st Century Act and set aside $2.7 billion for the program.

Issue 3: Microelectronics Education

Recommendation 2.6: Create a Scalable and Replicable Microelectronics Capable Workforce Development Model. This option provides a reliable, sustained pipeline of microelectronics capable workforce talent to the private sector—especially the aerospace and defense industry—and the United States Government. The Commission recommends that Congress authorize and fully fund the existing Private-Public-Academic-Partnership program in FY 2021 and expand it to include an AI-specific consortium in FY 2022.

Recommendation 2.7: Create a National Microelectronics Scholar Program. At $60 million per year, this program would tentatively produce 750 graduates a year with B.S., M.S., or Ph.D. EE/CE degrees. The Commission recommends that Congress authorize and fully fund a National Microelectronics Scholar Program.

LOE 4: Protect and Build on U.S. Technology Advantages

Progress to Date: The United States must promote and protect advantages in hardware to sustain its leadership in AI and associated technologies. In Q1, the Commission recommended investing in microelectronics leadership through the revitalization of domestic fabrication of state-of-the-art microelectronics. In Q2, the Commission focused on technology protection principles and recommendations for improving export controls and investment screening for emerging technologies.

TAB 4 — Protect and Build Upon U.S. Technology Advantages

Focus: AI exists within a constellation of emerging technologies. While AI is the lynchpin of this constellation given its ability to enable or be enabled by such a wide variety of technologies, their interconnected nature is why the Commission's mandate includes AI and "associated technologies." It is imperative that the United States continue posturing itself for a sustained technology competition that extends beyond AI and encompasses a broader suite of associated, emerging technologies.

Objective: The following recommendations pertain to steps the United States must take to ensure continued U.S. leadership in key technologies associated with AI, to include biotechnology, quantum computing, and microelectronics, as well as how the Executive Office of the President can better organize itself for technology competition.

Part I: Biotechnology

Recommendation 1.1: Prioritize U.S. Leadership in Biotechnology as a National Security Imperative and Pursue Whole-of-Government efforts to Support U.S. Biotechnology Advantages and Ensure the United States is a World Leader in Ethical Genomic Data Aggregation and Analysis. Given the ways in which AI will transform biotechnology applications, the United States Government must increase its support for the biological sciences, including funding for basic research, forecasting of future breakthroughs, and talent promotion efforts, to ensure continued U.S. leadership. It should specifically expand existing efforts which aggregate genetic data in a secure manner, such as the All of Us initiative, to enhance the ability of U.S. researchers to utilize AI for large-scale biotechnology research and innovation and reduce their reliance on Chinese entities for large-scale genomic research databases.

Recommendation 1.2: Increase the Profile of Biosecurity Issues and Biotechnology Competition within the U.S. National Security Departments and Agencies, Treat Chinese Advancements in Biotechnology as a National Security Priority, and Update the U.S. National Biodefense Strategy to Include a Wider Range of Biological Threats. The United States must treat China's attempts to gain strategic advantage by leveraging AI to achieve breakthroughs in biotechnology as a national security priority and increase the profile of and resource devoted to biosecurity and biotechnology issues in all U.S. national security departments and agencies. It should update the *National Biodefense Strategy* to include a wider vision of biological threats, such as AI-enabled human enhancement or how U.S. competitors could utilize biotechnology or biodata advantages as an instrument of national power.

Recommendation 1.3: Launch a Strategic Communications Campaign to Highlight BGI's Links to the Chinese Government and How China is Utilizing AI to Enable Ethically Problematic Developments in Biotechnology and Strengthen International Bioethical Norms and Standards Regarding Genomics Research. The United States should take a more aggressive public posture regarding BGI—China's de facto national champion in genetic sequencing and research—and senior officials should publicly highlight its links to the Chinese government and the national security risk that the company poses to the United States and its allies. Additionally, the United States should more aggressively highlight and condemn ethically problematic AI-enabled biotechnology research or applications by the researchers in China or the Chinese government, while simultaneously leading global efforts to emphasize and define bioethical guardrails for experiments involving AI applied to genetics and synthetic biology.

Recommendation 1.4: Pursue Global Cooperation on Smart Disease Monitoring. The United States should seek to collaborate with all nations to utilize AI to enhance global cooperation on disease monitoring. Such an international effort, which could combine data about zoonotic spillovers with other open-source data capable of estimating disease activity, would improve global pandemic defense while also providing an important model for large-scale global cooperation on AI toward issues of collective benefit.

Part II: Quantum Computing

Recommendation 2.1: Publicly Announce Government Interest in Specific Quantum Use Cases to Incentivize Transition from Basic Research to National Security Applications. In order to further practical applications of quantum technologies, the United States Government should consider publicly announcing a set of specific use cases for quantum computers that it is interested in pursuing. Public announcements of priority applications will help spur private sector investment and innovation in transitioning quantum technologies despite the absence of an integrated technology procurement apparatus within the United States Government.

Recommendation 2.2: Make Quantum Computing Accessible to Researchers via the National AI Research Resource. The United States should provide access to both classical and quantum computers via the National AI Research Resource, which the Commission recommended establishing in its *First Quarter Recommendations*. Doing so would help industry, academia, and government researchers build and test software tools and algorithms that leverage both classical and quantum computers in a hybrid fashion.

Recommendation 2.3: Foster a Vibrant Domestic Quantum Fabrication Ecosystem. Because quantum computing could exponentially increase the power of AI, the United States must take steps now to cement its long-term status as the global leader in the design and manufacturing of quantum processing units. Congress should enact a package of provisions that incentivizes the domestic design and manufacturing of quantum computers and their constituent materials, including tax credits and loan guarantees for relevant expenditures.

Part III: Microelectronics Leadership and Critical Technology Supply Chain Resilience

Issue 1: Developing a Resilient Domestic Microelectronics Industrial Base

Recommendation 3.1: Incentivize Domestic Leading-Edge Microelectronics by Authorizing and Fully Funding Key Provisions of the CHIPS for America Act, including the Advanced Packaging National Manufacturing Institute. To incentivize the development by the private sector of a state-of-the-art domestic commercial foundry, Congress should authorize and fully-funding provisions from the CHIPS for America Act (H.R.7178 / S.3933) included in the Senate and House versions of the NDAA via amendments. Key provisions would boost semiconductor research funding and development of advanced packaging and interconnect technologies and establish national centers of excellence for microelectronics and an incubator for semiconductor startup firms.

Recommendation 3.2: Create Private Sector Incentives for Developing a Leading-Edge Merchant Fabrication Facility Through Refundable Investment Tax Credits. Congress should pass legislation adopting a 40 percent tax credit on semiconductor manufacturing equipment and facilities for use in the United States through 2024. Closing the gap between U.S. tax rates on semiconductor capital equipment and other advanced industrial nations such as South Korea, Japan, and Taiwan will incentivize U.S. firms to construct facilities domestically while also attracting foreign firms such as the Taiwan Semiconductor Manufacturing Company.

Issue 2: Promoting Resilient Supply Chains for Critical Technologies

Recommendation 3.3: Improve Supply Chain Analysis, Reporting, and Stress Testing. The United States must establish a unit within NIST charged with understanding U.S. capabilities and gaps in domestic advanced technology production while also directing agencies to update their methodologies for collecting and publishing detailed supply chain data. The Federal Government should also work with industry to design and execute supply chain stress testing for companies in critical industries for national security, starting with microelectronics.

Recommendation 3.4: Centralize Reshoring and Supply Chain Management. The Executive Branch should bring together representatives from the Department of State, Defense, Commerce, U.S. Trade Representative, Small Business Administration, export promotion agencies, and others as needed into a fusion cell for reshoring and promote the resilience of critical elements of supply chains. As a next step, the recommendation also directs the Executive Branch to conduct an analysis of alternatives for organizations to lead domestic supply chain reshoring by drawing on expanded authorities and financial incentives, to include government agencies, consortia, and nonprofits.

Part IV: A Technology Competitiveness Council: Logic and Options

Recommendation 4.1: Develop a Comprehensive Technology Strategy and Empower an Entity within the White House to Ensure Continued Leadership Across Emerging Technologies. The United States must strengthen executive leadership in technology policy in the White House by empowering a single entity to develop a comprehensive technology strategy for the United States. The Commission offers a range of organizational models which could perform this function and recommends creating a new Technology Competitiveness Council chaired by the Vice President with an Assistant to the President serving as the day-to-day coordinator.

LOE 5: Marshalling International AI Partnerships

Progress to Date: The world is entering a dangerous period of international politics. International dialogue about the AI-enabled future must be part of any strategy, and cooperation even with competitors will be important in areas like smart disease monitoring. In Q1, the Commission proposed a National Security Policy Framework for AI Cooperation and recommended AI-related military concept and capability development with allies and partners, beginning with a focus on the Five Eyes alliance. In Q2, the Commission proposed reorienting the Department of State to lead coalitions of free and open states and organizations to prevail on emerging technology issues in an era of great power competition.

TAB 5 — Marshal Global AI Cooperation & Ethics

Focus: Leverage relationships with allies and partners, which represent asymmetric advantages over competitors/adversaries, to confront new threats and prevail over authoritarian regimes.

Objective: Identify opportunities for the United States to marshal global cooperation around AI & emerging tech to promote common interests and values of like-minded nations and to shape worldwide AI norms and use.

Pillar I: Deepening Global AI Coordination for Defense and Security

Recommendation 1: The Departments of State and Defense should provide clear policy guidance and resource support to NATO's AI initiatives by aligning resources and providing technical expertise to assist NATO in its adoption of AI to achieve: Accelerated development and adoption of operational practices to implement overarching AI principles and enable incorporation of AI-related technologies; Coordination of data sharing practices with a focus on privacy-enhancing technologies and methods; Development of NATO's technical expertise; Adoption of technical standards and architecture to promote interoperability; and Implementation of simulations, wargaming, experimentation, and pilot projects to develop use cases for data fusion, data exploitation, and interoperability across the Alliance. This recommendation focuses on steps that Departments of State and Defense should take to strengthen the ability of NATO—including the NATO Alliance and Allies—to develop and incorporate AI into operations consistent with the rule of law, the law of war, and democratic values. These steps include a recommendation for the Secretaries of State and Defense to issue a joint memorandum encouraging the Departments, as they liaise with NATO, to emphasize critical areas from the NSCAI's *Key Considerations* as strategic priorities for NATO member alignment. The Departments should elevate areas across the *Key Considerations* document as appropriate, while giving particular weight and emphasis to achieving common documentation requirements; establishing confidence in 'systems of systems'; and ensuring robustness and reliability, including mitigating adversarial machine learning attacks.

Recommendation 2: The Departments of State and Defense should negotiate formal AI cooperation agreements with Australia, India, Japan, New Zealand, South Korea, and Vietnam. This recommendation builds on growing support for the Quadrilateral Security Dialogue, a strategic forum among the US, Australia, India, and Japan, and calls for formalizing relationships with these and other nations in the Indo-Pacific region to focus on AI cooperation for defense and security purposes.

Pillar II: Shaping Global AI Cooperation through Multilateral Forums

Recommendation 3: The United States, through the Department of State, should lead in developing the international AI environment by working with partners and adopting a "coalition of coalitions" approach to multilateral efforts. This recommendation calls on the United States Government—led by the Department of State and coordinated through the proposed Technology Leadership Council—to engage proactively with promising multilateral efforts across the AI landscape that involve key partners and allies. It focuses on the following efforts: the OECD, the OECD AI Policy Observatory, the D-10 coalition, the Global Partnership for AI, new Department of State-led initiatives such as Clean Networks, and a new U.S.-India-Israel initiative as a potential model for additional focused efforts involving more than two nations. The report includes detail on a broad array of AI-related efforts and provides guidance for the United States Government to prioritize engagement with each.

Recommendation 4: The President, through the Department of State, should initiate efforts to establish a Digital Coalition of democratic states and the private sector to coordinate efforts and strategy around AI and emerging technologies, beginning with a Digital Summit. The Commission proposes a Digital Summit as a necessary step to coordinate with democratic allies and partners, identify gaps in existing projects, develop a shared research agenda, operationalize AI principles, and develop a stronger framework to safeguard against malign/adversarial uses of AI.

Recommendation 5: The President should issue an Executive Order to prioritize United States Government-efforts around technical standards through improved interagency coordination and improved collaboration with U.S. industry. This recommendation, if implemented, would establish an interagency coordination task force to promote collaboration with industry, direct federal agencies to resource international standardization efforts, and require NIST, through the Director of NIST and the Standards Coordinator, to encourage a private sector-created Standardization Center. These steps (and those in Recommendations 6-8) will strengthen United States Government and U.S. industry positions in international technical standards development.

Recommendation 6: Congress should appropriate funds to NIST and key agencies for a dedicated interagency AI standards team to support the U.S. AI Standards Coordinator. This recommendation reflects a need for the United States Government to have personnel dedicated to the international technical standards development processes. With a focus on U.S. national security, this recommendation calls for at least five full-time equivalent personnel at NIST and at least one each from the Departments of State, Defense, Energy, Homeland Security, ODNI, and other agencies as may be appropriate.

Recommendation 7: Congress should establish a Small Business Administration grant program to enable small- and medium-sized U.S. AI companies to participate in international standardization efforts. This recommendation would create a $1 million annual grant program to support engagement of small- and medium-sized U.S. AI companies in international technical standards development; this is a gap identified by industry and United States Government reps and is important as these companies are critical to developing new AI technologies and applications. Evaluation would be undertaken by the Small Business Administration in coordination with NIST.

Recommendation 8: Under NIST's lead, the United States Government, in coordination with U.S. industry and U.S. allies, should promote international standardization in areas that further U.S. and allies' national security and defense interests in the appropriate and responsible use of AI. This recommendation leverages NSCAI's *Key Considerations for Responsible Development & Fielding of AI* and focuses on United States Government input on national security-related needs, which is uniquely in the United States Government domain.

The Department of State's technology officers in international tech hubs should facilitate international alignment in coordination with NIST.

Pillar III: Building Resilient AI Cooperation with Key Allies and Partners

Recommendation 9: The United States should center its Indo-Pacific relationships around India including by creating a U.S.-India Strategic Tech-Alliance. This recommendation calls for the United States to center its Indo-Pacific relations around India with emerging tech as a key focal point; recognizing the importance of India as the world's largest democracy; the growing geopolitical challenges faced by India; the shared commitment to freedom, democratic principles, and the rule of law; and the many shared interests of the two nations, including strong innovation and technical infrastructures. The Department of State, in coordination with the Departments of Defense and Commerce, must lead the creation of the UISTA, —through high-level dialogues and regular working groups—should build on potential for strong collaborative work in the region for R&D, defense and security purposes, promoting innovation, strengthening talent exchanges and flows, and other aspects of the AI landscape. The Commission intends to provide a deep dive assessment of the potential for this Alliance in the final report.

Recommendation 10: The Department of State should create a Strategic Dialogue for Emerging Technologies with the European Union (EU). This recognizes the critical role of U.S.-EU relations across virtually all areas of emerging technology and international affairs, and calls for a Cabinet and Secretary-level Strategic Dialogue, accompanied by working group-level discussions, to further the relationship between the United States and EU, explore concrete avenues for collaboration, and address geopolitical challenges from a perspective of shared democratic values. The Commission intends to provide a deep dive assessment of the potential for deepening U.S.-EU relations around AI in the final report.

Recommendation 11: The United States Government, led by the Department of State, should engage in high-level and working group meetings with select key partners and allies on concrete, operational AI projects and applications and use the proposed Blueprint for AI Cooperation to assess and identify areas to deepen the relationship. The Commission proposes a Blueprint for AI Cooperation that includes concrete, operational guidance across eight critical areas: defense & security cooperation, standards & norms development, joint R&D, data-sharing ecosystem, innovation environment, human capital, countering information operations, & AI to benefit humanity. In the final report, the Commission intends to develop the Blueprint based on feedback and use it to assess and provide a roadmap for bilateral AI cooperation with India, the EU, and a number of other allies and partners.

LOE 6: Ethics & Responsible AI

Progress to Date: In the *2019 Interim Report*, the Commission argued that American AI must reflect American values, including the rule of law. The Commission also noted the basic convergence among national security officials and those in the AI development and ethics community on the need for trustworthy AI. The Commission has sought to provide recommendations on how to develop and field AI responsibly. Q1 recommendations focused on responsible AI training, documentation strategies, and the need for assessments of whether agencies are adequately relying on multidisciplinary analysis in AI procurement decisions. In Q2, the Commission issued a Key Considerations "paradigm" that includes 32 recommended practices across the AI lifecycle for the responsible development and fielding of AI.

TAB 5 — Marshal Global AI Cooperation & Ethics

Focus: The Commission recommends that the Departments of Defense and State elevate the Key Considerations paradigm in consultations with NATO, as a blueprint for how the alliance can put into practice overarching principles on the responsible development and fielding of AI.

Objective: To put into practice overarching principles on the responsible development and fielding of AI.

TAB 1 — Strengthening the Triangular Alliance for Artificial Intelligence (AI) Research and Development

Federal investments in Research and Development (R&D) helped end World War II, put the first man on the moon, maintain U.S. military advantages to win the Cold War, and set the stage for the information age with the invention of the Internet. Dr. Vannevar Bush, who oversaw wartime research and development through World War II, penned in a 1945 letter to President Roosevelt:

> *Without scientific progress the national health would deteriorate; without scientific progress we could not hope for improvement in our standard of living or for an increased number of jobs for U.S. citizens; and without scientific progress we could not have maintained our liberties against tyranny.*[1]

America's ability to harness innovation is predicated on a rich interplay between the triangular alliance of academia, government, and industry—and organizations that straddle those lines[2]—where each sector benefits from and relies on the advances of the others. Each has a role to play, and the level of progress and benefit to the broader society would not be achievable without strength across all pillars. GPS, touch screens, cloud computing, and Siri voice recognition capabilities all got their start in projects funded by the Defense Advanced Research Projects Agency (DARPA);[3] Tesla's battery technologies and solar panels came to fruition as a result of support from the Department of Energy (DoE);[4] DARPA partnered with Lockheed and Northrop to develop the stealth technology that provided U.S. aircraft an unparalleled advantage over competitors.[5]

The Federal Government plays a central role in supporting the basic and mission-driven research that sustains the United States' ability to push the limits of industrial progress, ensure national security competitiveness, and fuel a world-class academic training ground. As the world accelerates towards a future defined by emerging technologies such as AI and as America's strategic competitors and adversaries focus on closing the technological gap, the fundamentals of this alliance and its centrality for U.S. technological leadership do not change.

[1] Vannevar Bush, *Science: The Endless Frontier,* United States Government Printing Office (1945), https://nsf.gov/od/lpa/nsf50/vbush1945.htm.

[2] For example, Federally Funded Research and Development Centers based at universities conduct sensitive government-sponsored research and maintain domain expertise in national security application areas, and not for profit research organizations such as Draper Laboratories or SRI International operate outside of academia in support of both government and industry.

[3] Phil Goldstein, *The 5 Most Amazing Technologies DARPA Helped Invent — Besides the Internet,* FedTech (Apr. 29, 2016), https://fedtechmagazine.com/article/2016/04/5-most-amazing-technologies-darpa-helped-invent-besides-internet.

[4] Rana Foroohar, *Why You Can Thank the Government for Your iPhone*, TIME (Oct. 27, 2015), https://time.com/4089171/mariana-mazzucato/.

[5] John T. Correll, *History of Stealth: From Out of the Shadows*, Air Force Magazine (Sept. 1, 2019), https://www.airforcemag.com/article/history-of-stealth-from-out-of-the-shadows/; Ian A. Maddock, *DARPA's Stealth Revolution*, DARPA (Jan. 1, 2008), https://www.darpa.mil/attachments/(2O24)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Stealth%20(Approved).pdf.

However, the level and manner in which the Federal Government bolsters this advantage will determine the nation's ability to harness AI for future economic prosperity and national security competitiveness. To support the level of AI research, development and application that will underpin future U.S. technological leadership, the government must act. It should strengthen the alliance by exploring new mechanisms to support research and enable partnerships with industry, and put the national security research and development community on a footing that enables transition of advancements from open research into secure, modern environments that facilitate collaboration with a range of internal and external actors.

Opportunities exist to leverage the triangular alliance to build future national security capabilities in a multitude of AI research areas, notably human-AI teaming, adversarial AI, and trustworthy AI. Collaboration can also further the research priorities the Commission underscored for the non-defense community in the Commission's First Quarter recommendations: novel machine learning directions; testing, evaluation, verification, and validation (TEVV) of AI systems; robust machine learning; complex multi-agent scenarios; AI for modeling, simulation, and design; and advanced scene understanding.[6]

In the Commission's *2019 Interim Report* to Congress, NSCAI found that the United States Government should implement more flexible funding mechanisms to support AI as well as look into opportunities to establish a nationwide AI R&D infrastructure.[7] In its *Second Quarter Recommendations*, the Commission found that researchers within the Department of Defense (DoD) were limited in their ability to innovate in AI by outdated processes, funding policies, and organizational cultures.[8]

In order to strengthen the triangular alliance and position the United States for an AI-enabled future, the Commission recommends actions to address three priority issue areas:

1. Supporting the growth of nationwide AI R&D through novel funding mechanisms;

2. Posturing the defense and intelligence AI R&D communities to address national-security specific problems and capabilities through establishment of a modern digital ecosystem; and

3. Expanding the role of industry in DoD's AI R&D to pursue next-generation capabilities.

Through focused attention and strategic application of resources, the Commission believes the Federal Government can harness U.S. innovation to use AI to solve near term challenges encountered by U.S. warfighters, intelligence analysts, and national security professionals, as well as those of the business enterprises of the agencies that house them; and build over-the-horizon capabilities that will underpin a future U.S. competitive advantage.

[6] *First Quarter Recommendations*, NSCAI at 11 (Mar. 2020), https://www.nscai.gov/reports.
[7] *Interim Report*, NSCAI at 27-28 (Nov. 2019), https://www.nscai.gov/reports.
[8] *Second Quarter Recommendation*, NSCAI at 1 (July 2020), https://www.nscai.gov/reports.

Issue 1: Supporting AI Research through Novel Funding Mechanisms

In the *2019 Interim Report*, the Commission found that for the United States Government to support the level of AI research needed to transform U.S. society, economy, and national security, business as usual is insufficient. The Commission assessed that the United States Government retains a pivotal responsibility to support basic scientific research as well as research that is directly relevant to national security; and that, like the transformational technologies that came before it, AI will reach its fullest potential when supported by government investments.[9]

The traditional federal short-term, project-based grants, while crucial to spur inquiry into novel technology and methods, are not in themselves sufficient to unlock transformational, widespread innovation. To maximize the ability of federal research funding to significantly impact the field, the government should pursue a portfolio approach that leverages a diverse set of mechanisms, focused on a range of outcomes—be that advancement of basic science, solving specific challenge problems, or facilitating commercialization of breakthroughs.

In the case of AI, traditional federal research support often falls short given the need for capital-intensive computation, specialized data sets, and data storage; and for larger-scale ambitions, engineering support from software and hardware engineers. The Commission's first quarter recommendation to Congress to launch a pilot of a National AI Research Resource to provide researchers and students low-cost access to compute, co-located with AI-ready data sets and user training, was an initial step toward addressing this deficiency and supporting foundational AI research nation-wide.[10]

The Commission applauds the recent steps the Federal Government has taken to support AI research at higher levels and through new mechanisms. Notable among these efforts include DARPA's Artificial Intelligence Exploration Program, which fast tracks funding for awards up to $1 million to explore feasibility of new AI concepts within an 18 month timeframe;[11] and the National Science Foundation's (NSF's) National AI Research Institute effort, which has this year funded seven multi-institution, university-based research institutes at $4 million per year for five years, and plans to launch another eight next year.[12] Furthermore, under the banner of the American AI Initiative, the Administration has committed to doubling non-defense funding for AI R&D by Fiscal Year 2022 to $2 billion.[13]

[9] *Interim Report*, NSCAI at 24-25 (Nov. 2019), https://www.nscai.gov/reports.

[10] *First Quarter Recommendations*, NSCAI at 12-13 (Mar. 2020), https://www.nscai.gov/reports.

[11] This program, focused on "third wave AI", constitutes a series of unique funding opportunities that use streamlined contracting procedures to achieve a start date within three months and evaluation of a concept in 18 months. See *Accelerating the Exploration of Promising Artificial Intelligence Concepts*, DARPA (July 20, 2018), https://www.darpa.mil/news-events/2018-07-20a.

[12] *Artificial Intelligence at NSF*, NSF (Aug. 26, 2020), https://www.nsf.gov/cise/ai.jsp. The first round of seven institutes are organized around the research areas of: Trustworthy AI; Foundations of Machine Learning; AI-Driven Innovation in Agriculture and the Food System; AI-Augmented Learning; AI for Accelerating Molecular Synthesis and Manufacturing; and AI for Discovery in Physics. The National AI Research Institutes initiative is a joint effort of the National Science Foundation, U.S. Department of Agriculture's National Institute of Food and Agriculture, U.S. Department of Homeland Security's Science & Technology Directorate, U.S. Department of Transportation's Federal Highway Administration, and U.S. Department of Veterans Affairs. Id.

[13] NSCAI has called for an immediate doubling of funding in Fiscal Year 2021. The Networking and Information Technology Research and Development Program's supplement to the President's Fiscal Year 2021 budget

However, as the Association for the Advancement of AI stated in its *20 Year Community Roadmap for Artificial Intelligence:* "Achieving the full potential of AI technologies poses research challenges that require a radical transformation of the AI research enterprise, facilitated by significant and sustained investment."[14]

These investments should create a vibrant fabric of funding, both mission-oriented and investigator-driven, that balances sustainment of evolutionary progress with bets on revolutionary breakthroughs, as well as theoretical exploration with applied problem solving and practical pathways to expedite commercialization. The Commission recommends the following five actions to strengthen federal support for the AI R&D environment alongside ongoing R&D funding.

Recommendation 1: Create an AI Innovator Award Program to Invest in Top Talent

Top talent in AI is a scarce commodity. The Commission's *2019 Interim Report* identifies talent as a lynchpin in the strength of the U.S. AI research environment and in the nation's ability to maintain technological leadership on the world stage.[15] Due to the scarcity of AI talent globally and the growing recognition that AI is a key technology for economic and national security, talent has become a critical facet of international competition.[16]

Investing in talent holds the potential to not only unlock breakthroughs in the science and application of AI but also attract and retain top talent in the United States.[17] As the Commission has heard from a range of AI researchers: "talent follows talent." Thus, a

reports a total requested interagency investment in AI R&D of $1.5 billion. See *AI R&D Investments*, The Networking and Information Technology Research and Development Program (Aug. 14, 2020), https://www.nitrd.gov/apps/itdashboard/AI-RD-Investments/#AIpiechart.

[14] Yolanda Gil & Bart Selman, *A 20-Year Community Roadmap for AI Research in the US, Computing Community Consortium and Association for the Advancement of Artificial Intelligence*, CCC & AAAI at 2 (Aug. 6, 2019), https://cra.org/ccc/wp-content/uploads/sites/2/2019/08/Community-Roadmap-for-AI-Research.pdf.

[15] NSCAI's Line of Effort on workforce has advanced a suite of recommendations in quarters 1 and 2 to strengthen the AI workforce in government, to include expanding federal technology scholarship for service programs, increasing partnerships with industry, establishing a National Reserve Digital Corps, and launching a U.S. Digital Service Academy.

[16] Since 2008, China has launched a series of talent-focused programs, aimed at attracting STEM talent—both foreign and returning expatriates—to work in China. Estimates put the number of such programs at more than 200. See Staff Report, *Threats to the US Research Enterprise: China's Talent Recruitment Plans*, Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations at 20-22 (Nov. 18, 2019), https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China%27s%20Talent%20Recruitment%20Plans.pdf. NSCAI has launched a special project to tackle the interrelated priorities of competing for top international talent and protecting the U.S. research environment from China's technology transfer initiatives such as talent recruitment programs.

[17] A 2019 evaluation of the grants made as a component of the National Institutes of Health (NIH) high-risk, high-reward program—which include large, longer term investments in talent through the NIH Director's Pioneer Award, NIH Director's New Innovator Award, and the NIH Director's Early Independence Award—found that these awards funded highly productive research compared to the work funded under traditional NIH research grants and that they result in a higher technological impact. The high-risk, high-reward program was created to accelerate the pace of biomedical, behavioral, and social science discoveries by supporting creative scientists with highly innovative research. See *Report of the ACD Working Group on High-risk, High-reward Research*, National Institutes of Health Advisory Committee to the Director (June 2019), https://www.acd.od.nih.gov/documents/presentations/06132019HRHR_B.pdf.

talent-focused effort brings an added benefit by building communities of innovation in U.S. academic institutions.

As the President's Council of Advisors on Science and Technology asserted in a report on the future of the U.S. research environment: "The largest returns of research often come from unexpected new discoveries that open up whole new vistas."[18] The Commission recommends the launch of an AI innovator program to create a mechanism that provides top researchers the flexibility to pursue big ideas without prescribed outcomes, and the United States Government an ability to balance ongoing investments in incremental progress with bets on revolutionary breakthroughs.

Administered by an independent non-profit entity funded by the government and overseen by NSF,[19] an AI Innovator Award would be loosely modeled on that of the National Institutes of Health (NIH) Pioneer Award[20] and the storied Howard Hughes Medical Institute (HHMI), both designed to foster high-risk exploratory research.[21] A 2011 study of the program found that HHMI investigators published high-impact papers at a significantly higher rate than similarly-accomplished scientists funded by traditional NIH grants, and that their research more often tackled novel topics.[22]

Rather than the traditional approach of a grant awarded for a defined research project focused on a specific outcome, the AI Innovator Award would represent investment in a

[18] *Report to the President Transformation and Opportunity: the Future of the US Research Enterprise*, President's Council of Advisors on Science and Technology (Nov. 2012), https://www.broadinstitute.org/files/sections/about/PCAST/2012%20pcast-future-research-enterprise.pdf.

[19] This could be conducted through a cooperative agreement, mirroring the relationship the National Science Foundation formed with the Computing Research Association to launch the Computing Innovation Fellows program in 2009 to support post-doctoral PhDs imperiled in finding academic appointments by the downturn of the economy. See *CIFellows*, Computing Community Consortium (last accessed Sept. 3, 2020), https://cra.org/ccc/leadership-development/cifellows/. The non-profit would act independent of NSF in terms of selection of awardees, and would be able to accept supplemental funding from individuals, corporations, or other non-profits to further strengthen and expand the program.

[20] The NIH Director's Pioneer Award, established in 2004, supports researchers at any career stage who propose bold research projects with unusually broad scientific impact. The program seeks to identify scientists with high-impact ideas that may be risky or at a stage too early to fare well in the traditional peer review process, and supports awardees with $3.5 million over 5 years, and require 51 percent of time spent on research in the first three years. See *NIH Director's Pioneer Award*, National Institutes of Health (Aug. 26, 2020), https://commonfund.nih.gov/pioneer. Competition for participation in the program is high, reportedly success rate for applicants is just 1 percent. See Roberta B. Ness, *The Creativity Crisis*, Oxford University Press at 88 (2015), https://books.google.com/books?id=woYeBQAAQBAJ&pg=PA87&lpg=PA87&dq=hhmi+funding+model&source=bl&ots=apcet-3WYF&sig=ACfU3U3Hc32rLoM2ASTTVfdYtuCy8C1PXg&hl=en&sa=X&ved=2ahUKEwir6dK_y4fkAhUprlkKHfG_D1U4ChDoATAFegQICRAB#v=onepage&q=hhmi%20funding%20model&f=false.

[21] Established in 1978, the Howard Hughes Medical Institute (HHMI) supports over 250 investigators across the United States. 30 current or former HHMI investigators have been awarded the Nobel Prize. The HHMI Investigator Program is organized around the core belief in the power of individuals to make breakthroughs over time. Through the program, which selects 20 investigators per year, HHMI aims to expand a community of basic researchers and physician scientists who catalyze discovery research in basic and biomedical sciences, plant biology, evolutionary biology, biophysics, chemical biology, biomedical engineering, and computational biology. See *Competition to Select New HHMI Investigators*, HHMI (2020), https://www.hhmi.org/sites/default/files/programs/investigator/investigator2021-program-announcement-200714.pdf.

[22] Pierre Azoulay, et al., *Incentives and Creativity: Evidence from the Academic Life Sciences*, NBER (Dec. 2011), https://www.nber.org/papers/w15466.

person—a researcher who has potential to push the frontiers of the field.[23] The award would support the work of select researchers for a term of five years, allowing them the freedom to pursue high-risk research and redirect focus as warranted by their investigations. The award would be granted based on a proven track record of prior innovation and the researcher's proposed general research program—which would be understood as subject to change and redirection.

Selection for the award would be conducted by a small, rotating panel of AI experts, who would provide meaningful feedback to selectees throughout their participation in the program.[24] To ensure selection of innovative candidates, the panel should follow an advocacy model, where candidates are ranked in accordance with the maximum scores provided by reviewers, thereby placing priority on their upside potential.[25]

Each year, this panel would select between 10 to 20 recipients for five-year terms, which would be renewable at the close of the five-year term. Totaling around $5.5 million per awardee for the five-year term, the awards would cover the full salary and benefits of the researchers at their respective institutions as well as provide a research budget that would support research equipment and staff.[26] Researchers would be eligible to apply for additional funding from the program to support major equipment investments.

Eligible researchers would be those at any career stage based at U.S. universities or research institutions who commit to spending 75 percent of their time on research.[27] Attention should be paid by the selection panel to the need for diversity among awardees—in terms of gender, race, age, location, and primary focus area of study; as well as on the communication and leadership skills of applicants. At the end of their five-year term, researchers would be eligible to apply for renewal.

[23] In our *First Quarter Recommendations*, NSCAI recommended a 10% funding increase in a range of DoD, DOE, NASA, and NSF fellowship and talent programs to support AI-specific work. NSF manages a suite of programs targeting talent, from undergraduate and graduate fellowships to early career funding. The primary NSF effort under this umbrella is the Faculty Early Career Development (CAREER) program, which supports promising early-career faculty at around $500k over five years and includes an educational component. These awards are made across NSF directorates. See *Faculty Early Career Development Program (CAREER)*, NSF (last accessed Sept. 29, 2020), https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503214. Particular to AI is a complementary program out of NSF's Computer and Information Science and Engineering directorate that grants early career, untenured academics within three years of their PhD completion a 24 month award of $175k to provide early support to launch a research initiative. See *Computer and Information Science and Engineering Research Innovation Initiative*, National Science Foundation (last accessed Sept. 29, 2020), https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504952.

[24] The quality of feedback provided by reviewers was identified by Azoulay et al, as a key factor in the success of HHMI investigators. Pierre Azoulay, et al., *Incentives and Creativity: Evidence from the Academic Life Sciences*, NBER (Dec 2011), https://www.nber.org/papers/w15466.

[25] Pierre Azoulay & Danielle Li, *Scientific Grant Funding*, MIT & NBER (Mar. 2020), https://mitsloan.mit.edu/shared/ods/documents/?PublicationDocumentID=6296. See also the "gold award" model used by the Bill and Melinda Gates Foundation. *How Grand Challenges Explorations Grants are Granted*, The Gates Foundation (Sept. 3, 2020), https://gcgh.grandchallenges.org/how-grand-challenges-explorations-grants-are-selected.

[26] This mirrors the HHMI structure and cost model, with HHMI awarding $8 million over a seven-year term. HHMI updated the length of their award in 2018, extending the term length from five to seven years. See *HHMI Bets Big on 19 New Investigators*, HHMI (May 23 2018), https://www.hhmi.org/news/hhmi-bets-big-on-19-new-investigators.

[27] Should researchers move institutions over the course of the program, the award would move with them.

Participating researchers would be eligible to pursue supplementary government research grants to support graduate students working with them, provided that administrative obligations in the application and maintenance of the grant do not detract from the researcher's commitment to 75 percent time spent on research. Similarly, research support provided by individuals, non-profits, and corporations would be allowable, provided that gift and grant agreement provisions do not limit activities of the researcher nor assign sole ownership intellectual property rights to that supplemental funder. Commercialization of technology developed from a researcher's work would be subject to the provisions of the Bayh-Dole Act and the conflict of interest policy of the researcher's institution.[28]

Researchers in the program would participate in an annual meeting in which they would share their work, providing a venue for meaningful feedback between review cycles and helping build a community of innovation among the top U.S.-based minds in AI. The program would support a maximum of 100 researchers at a time, reaching an annual funding level of around $125 million for research support, with additional funds available for major equipment support.

Proposed Legislative Branch Action

The Commission recommends that Congress direct and fund NSF to partner with a non-profit organization to establish an AI Innovator Award to cultivate the next leaders in the field of AI in a manner that gives them the space to pursue research that can unlock transformative breakthroughs in AI. An innovator program would additionally help strengthen U.S. universities by covering the salary and research costs of the kind of top talent that brings prestige and attracts additional talent to the institution.

Congress should include in authorizing language a requirement to conduct an assessment of the program after seven years of operation to determine whether the program should continue to expand or operate at a lower number of awards, and to evaluate the impact of the funding level and award term on the research conducted by participants.

Recommendation 2: Invest in Research Teams Pursuing Transformative Ideas in AI

The goal of the AI Innovator program to make "big bet" investments in people and spark breakthrough research should be complemented with support for teams of researchers tackling big challenge problems through novel research initiatives. Studies have found that research that effectively combines diversity of knowledge is more likely to prompt breakthroughs,[29] and that interdisciplinary research lends itself to complex problem solving, developing new research thrusts, and challenging the status quo.[30] However, analysis of

[28] Passed in 1980, the Bayh-Dole Act created a uniform policy across federal grantmaking agencies that allows for institutions receiving grants to retain the title to patents resulting from government-funded research and license those rights to the private sector for commercialization. The Federal Government retains a royalty-free license to the technology, for use for a governmental purpose. See 35 U.S.C. Ch. 18, Patent Rights in Inventions Made with Federal Assistance (1980), https://uscode.house.gov/view.xhtml?path=/prelim@title35/part2/chapter18&edition=prelim.

[29] Lee Fleming, *Recombinant Uncertainty in Technological Search,* Management Science 47:1 (2001).

[30] Andrew Barry et al., *Logics of Interdisciplinarity*, Economy and Society 37:1 (Feb. 2008).

government funding portfolios also demonstrates that such scientifically-diverse teams are less likely to receive grant funding.[31]

A team award would focus on supporting bold research initiatives to apply AI to solve complex problems or to pursue use-inspired basic research efforts, which advance a fundamental understanding of the science while resulting in immediate benefit to society.[32] Either objective will benefit from effectively harnessing multidisciplinary research teams to work collaboratively towards novel solutions. Administered through a nonprofit overseen by NSF, the same partner as the AI Innovator program, selection would be conducted by the same panel, choosing 5-10 teams for non-renewable five-year terms. Teams would be awarded $4-$10 million per year for the five-year term of the award,[33] and would participate in the annual meeting of the AI Innovators to share the progress of their work. The program would have a starting annual budget of $50 million, reaching a height of $250 million.

Such a program should pull successful traits from the team-based approach often employed by DARPA,[34] as well as the NIH Transformative Research Award, the NIH National Institute of General Medical Sciences (NIGMS) Collaborative Program Grant for Multidisciplinary Teams, and the DoD Multidisciplinary University Research Initiative (MURI). The NIH Transformative Research Award places emphasis on supporting unconventional research—be it by an individual or team—with the potential to create new scientific paradigms, establish entirely new clinical approaches, or develop transformative technologies.[35] The NIGMS Collaborative Program Grant for Multidisciplinary Teams makes clear that "teams are expected to accomplish goals that require considerable synergy and managed team interactions" and "[p]roject goals should not be achievable with a collection of individual efforts or projects."[36] The DoD's MURI program similarly focuses specifically on leveraging multidisciplinary teams to generate novel approaches around designated DoD priority areas.[37]

[31] Albert Banal-Estanol, et al., *Key Success Drivers in Public Research Grants: Funding the Seeds of Radical Innovation in Academia?*, CESifo Working Paper Series 5852 (Mar. 2016).

[32] As argued by Donald Stokes in 1997, research should be conceived not as a dichotomy between basic and applied research, but on a quadrant along the axes of "quest for fundamental understanding" and "consideration of use." Research in the upper right quadrant is defined as use-inspired basic research—research that advances fundamental knowledge but is driven by a clear purpose. Stokes calls this "Pasteur's quadrant" after the work of Louis Pasteur, whose research pushed scientific boundaries and had practical applications. See Cherie Winner, *Pasteur's Quadrant*, Washington State University Magazine (2009), https://magazine.wsu.edu/web-extra/pasteurs-quadrant/.

[33] Amount of award would be adjusted in accordance with the specificities of the project. Eligible teams would be composed of researchers based in U.S. academic or research institutions proposing innovative work related to AI.

[34] Such as DARPA's Defense Sciences Office, which pursues multidisciplinary approaches for radical outcomes through the teaming of universities, service and federal laboratories, small businesses, and large industry. Lawrence H. Dubois, *DARPA's Approach to Innovation and Its Reflection in Industry,* National Research Council Chemical Sciences Roundtable, National Academies Press (2003), https://www.ncbi.nlm.nih.gov/books/NBK36337/.

[35] The awards are for $3.5 million for 5 years, with 51% of researcher time required to be spent on research. See *NIH's Director's Transformative Research Award*, National Institutes of Health (July, 7 2020), https://commonfund.nih.gov/tra.

[36] NIGMS supports 4-6 of the team awards each year, allowing applicants to request up to $1.5 million per year in direct cost budgets for up to 5 years. See *Collaborative Program Grant for Multidisciplinary Teams (RM1)*, U.S. Dept. of Health and Human Services (last accessed Sept. 15, 2020), https://grants.nih.gov/grants/guide/pa-files/PAR-17-340.html.

[37] Awards are for $1.5 million per year for 5 years. See *Fiscal Year 2020 University Research Funding Awards*, U.S. Department of Defense, Undersecretary of Defense for Research and Engineering (Sept. 3, 2020), https://www.cto.mil/2020-muri/.

Proposed Legislative Branch Action

The Commission recommends Congress direct and fund NSF to partner with a non-profit organization to establish a team-based AI research award with an annual budget of $50 million as a complement to the AI Innovator Award to encourage the application of AI to new fields and problem sets—accelerating breakthroughs while continuing to push the bounds of the technology.

Recommendation 3: Create AI Testbeds to Serve the Academic and Industry Research Communities

It's now well understood that training data and access to computation is critical for supervised machine learning. In the Commission's *First Quarter Recommendations,* the Commission recommended establishment of a National AI Research Resource to democratize access across the research community to compute power co-located with data sets. However, there are a range of shared resources that have the potential to accelerate progress in AI. For example, in reinforcement learning, an agent learns through interactions with the environment. Many researchers have used games to train agents, but more diverse and sophisticated environments will be needed for the development of real-world applications of reinforcement learning, as well as deterministic approaches, knowledge-based systems and the broad range of AI methods that will drive the future of the technology.[38] Research at the intersection of AI and cyber-physical systems will benefit from real-world testbeds. For example, the Autonomous Greenhouse Challenge allowed researchers to develop algorithms that increased the productivity and sustainability of indoor agriculture.[39]

To create a pull for innovation and fuel R&D in AI, the Commission recommends development of a set of national AI testbeds that would provide ready infrastructure, benchmarking standards, and build communities of discovery and practice around application areas for AI that are in the public interest.

These open resources would support the AI research community—not only in academia but also at small companies and in the United States Government. The testbeds would lower the cost of collaboration across multi-institution and multidisciplinary teams and provide training opportunities for students. Furthermore, they would help establish and maintain benchmarking standards that enable measurable research progress through comparison of approaches and reproducibility testing.[40]

Such resources should create environments that capture real-world dynamics, facilitating progress towards robust, usable systems. Supported by simulated, live, and blended environments, these platforms would support research and experimentation that tackles open-ended, real-world problems. Furthermore, they should be architected to collect

[38] See discussion of the diversity of AI approaches in *Interim Report*, NSCAI at 53 (Nov. 2019), https://drive.google.com/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view.
[39] See *AI beats growers in Autonomous Greenhouse Challenge 2020*, HortNews (June 10, 2020), https://hortnews.com/ai-beats-growers-in-autonomous-greenhouse-challenge-2020/.
[40] For a discussion of the benefit of testbeds to enable significant measurable progress, see Yolanda Gil & Bart Selman, *A 20-Year Community Roadmap for AI Research in the US*, Computing Community Consortium and Association for the Advancement of Artificial Intelligence at 91 (Aug. 6, 2019), https://cra.org/ccc/wp-content/uploads/sites/2/2019/08/Community-Roadmap-for-AI-Research.pdf.

valuable data that could be made accessible to the community for training and evaluation, providing additional fuel for progress.[41]

Investment in this suite of AI testbeds should be made across multiple Federal agencies, facilitating creation of domain-specific resources open to the broader research community. Testbeds should support experimentation with both novel software and hardware in live and virtual environments, equipped with rich simulation capabilities to model the physical world. For example, a self-driving vehicle test range, an instrumented humanitarian aid and disaster relief test site, or an instrumented home environment could all serve to advance critical areas of AI application.

Opportunities to create resources that can advance priority AI research areas include those focused on elements of adversarial AI, human-AI teaming, and AI-enabled robotics, as well as those that could support the focus areas of the NSF's growing network of National AI Institutes.[42] In addition, the priority areas noted by NSCAI in its *First Quarter Recommendations* of novel machine learning directions; testing, evaluation, verification, and validation; robust machine learning; complex multi-agent scenarios; AI for modeling, simulation, and design; and advanced scene understanding.

Attention should focus on modernizing existing resources to support data-driven and AI-enabled technologies. For example, AI testbeds could be hosted by DoE's existing national laboratory facilities and high-performance computing resources or by DoD's existing testing and evaluation infrastructure, or facilities managed by the Department of Transportation, National Institutes of Health, National Institute of Standards and Technology (NIST), or Department of Agriculture.

These would serve as steady, long-term resources that would support the entirety of the AI research community and provide shared platforms for translation of research to real-world applications. The effort should begin with establishment (or modernization) of 5-10 facilities that could support experimentation with software and hardware in live, virtual, and blended environments. The National Science and Technology Council (NSTC) Select Committee on AI, which holds the responsibility to "improve the overall effectiveness and productivity of Federal research and development (R&D) efforts related to artificial intelligence (AI)," should steward and coordinate investments to support alignment with national priorities.[43]

[41] Similar to existing NIST testbeds, these facilities should have online data streaming, collection, storage and publication services that provide real-time, universally compatible data links for experimenting; and a searchable repository of all data generated.

[42] NSF funded the first National AI Institutes this year on the topics of: Trustworthy AI in Weather, Climate, and Coastal Oceanography; Foundations of Machine Learning; Student-AI Teaming; AI for Molecular Discovery, Synthetic Strategy, and Manufacturing; AI and Fundamental Interactions; AI for Next Generation Food Systems; and AI for Future Agricultural Resilience, Management, and Sustainability. As well as those planned for 2022: Human-AI Interaction and Collaboration, Advances in Optimization, AI and Advanced Cyberinfrastructure, Advances in AI and Computer and Network Systems, Dynamic Systems, AI-Augmented Learning, AI to Advance Biology, AI-Driven Innovation in Agriculture and the Food System. See *Artificial Intelligence at NSF*, National Science Foundation (Sept. 3, 2020), https://www.nsf.gov/cise/ai.jsp.

[43] *Charter of the National Science And Technology Council Select Committee On Artificial Intelligence*, Executive Office of the President (May 9, 2018), https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf?latest#page=13.

Proposed Executive Branch Action

The Commission recommends the NSTC Select Committee on AI coordinate agency investments in AI testbed facilities through the annual budget request process, thereby enabling the AI research community through a network of national resources that would provide common means of testing and benchmarking performance of AI applications for real world uses. Focus areas of each testbed should be aligned with priority AI research areas and in support of existing Federal AI investments, help establish standards in the field, and move the community towards research that produces robust applications that translate to high-impact real-world solutions.

Recommendation 4: Support AI Data Set Curation and Maintenance

The recent acceleration of breakthroughs in computer vision and deep learning can be in part traced back to the creation of the ImageNet data set by Dr. Fei-Fei Lee in 2009.[44] Following the performance breakthroughs achieved with neural networks trained on a labeled data set the size of ImageNet, data has become a central currency in today's popular AI approaches.

Promising work in the realm of low-shot learning, semi-supervised learning, and learning from synthetic data provide glimpses of a future where performance of an AI system is not directly tied to big data, and the Federal Government should continue to prioritize funding for research in these areas. However, balancing these bets on the future with investments in resources to further U.S. leadership in the current leading AI approaches would strengthen the foundation of both current and future AI-based technology and applications.

Building AI systems and solutions for new domains and application areas relies on availability of specialized data that have been cleaned and organized for use. Federal support for well-designed, publicly-available data sets would help drive research progress in AI and its application to other fields of study.[45] Funding the curation, hosting, and maintenance of complex data sets would set the foundation for future AI capabilities, and help strategically steer the research community towards issues in the public interest, beyond bounded classification problems.

The DoE is well placed to manage such a program, leveraging the cross-disciplinary expertise resident throughout the laboratory network, the unique computing and user facilities housed at the 17 laboratories, and ability to create and maintain secure data environments.[46] It could build on promising data sharing efforts underway[47] as well as on

[44] Dave Gershgorn, *The Data that Transformed AI Research—and Possibly the World*, Quartz (July 26, 2017), https://qz.com/1034972/the-data-that-changed-the-direction-of-ai-research-and-possibly-the-world/; *About ImageNet*, ImageNet (2016), http://imagenet.stanford.edu/about-overview.

[45] The Commission's first quarter recommendation for a National AI Research Resource focused on providing the research community access to existing government and non-government data sets, co-located with computing resources. See *First Quarter Recommendations*, NSCAI at 12-13 (Mar. 2020), https://www.nscai.gov/reports.

[46] *User Facilities at a Glance*, Dept. of Energy Office of Science (last accessed Sept. 29, 2020), https://science.osti.gov/User-Facilities/User-Facilities-at-a-Glance#0.

[47] The program could build on the pathfinder Open Data Initiative launched by Lawrence Livermore National Laboratory in partnership with the University of California San Diego, which hosts complex, labelled data sets for testing solutions for scalable machine learning platforms. See *New Partnership Results in Increased Access to Compelling "Real World Data"*, The Library UC San Diego (Apr. 21, 2020),

existing cooperative relationships with universities and commercial sector partners. DoE should then work closely with NIST to develop standards for the data—to include standards for documentation, data modeling, data engineering, and data formats as well as to advance the methods and tools necessary to support the data lifecycle.

Driven by priority AI research areas coordinated by NSTC, emphasis should be placed on the creation of exemplar, complex data sets that would be maintained as living, regularly updated resources. These could include specialized data sets in physical, biological, earth, and engineering sciences, as well as in social sciences to support economic and behavioral studies.

These data investments could be further augmented by and created in support of the domain testbeds recommended above as well as NSF's seven National AI Institutes. This integration could foster creation of data sets to support benchmarks within the testbeds as well as generate rich data from testing that could be provided back out to serve the research community. Access to all resources should be granted to researchers with verified research efforts and governed by appropriate compliance controls based on the type of data contained in the data set.[48]

Proposed Legislative Branch Action

The Commission recommends Congress appropriate $25 million[49] per year for the next five years to DoE to administer an AI data program that would vector the AI research community towards real-world goal accomplishment by facilitating learning on rich, relevant data; support the application of AI to other fields of science; and advance technology around data set lifecycle maintenance. Strategic direction of the program should be overseen by the NSTC Select Committee on AI to ensure data sets supported steer the research community in desired directions.

https://library.ucsd.edu/news-events/new-partnership-results-in-increased-access-to-compelling-real-world-data/; *Open Data Initiative*, Data Science Institute (last accessed Sept. 29, 2020), https://data-science.llnl.gov/open-data-initiative.

[48] This could be integrated into and facilitated by the National AI Research Resource previously recommended by the Commission. See *First Quarter Recommendations*, NSCAI at 12-13 (Mar. 2020), https://www.nscai.gov/reports.

[49] This would provide for creation of five initial datasets, as well as maintenance over their lifetime and creation of additional data sets as the program matures.

Recommendation 5: Launch an AI Research Challenge

Research challenges and competitions are proven mechanisms to drive progress around key technologies.[50] The Federal Government has successfully used grand challenges[51] in the past to foster innovations that hold high return for the public good, most notably the Human Genome Project.[52]

The Institute for Defense Analyses defines the hallmarks of grand challenges as including "a pioneering vision, a large-scale collaborative effort, an ambitious but concrete target, and a flexible framework."

DARPA harnessed the challenge model in 2004 with its Grand Challenge that significantly expedited development of the technology that now underpins autonomous vehicles in development for commercial and military applications. DARPA has since continued this competition model to address reliable radio communication in congested environments, robots for disaster response, the power of social media networks, and fully automated cyber defense.[53]

To unlock new AI technologies to bolster the U.S. economy and defense capabilities, DARPA should launch a challenge around an ambitious AI-enabled goal that would drive the research community.[54] The challenge should focus on accelerating progress on third wave AI capabilities and advancing technology that could plausibly drive future defense and broader national security capabilities by focusing the community on an aspirational challenge that addresses a greater public good.

[50] For example, Xprize, a non-profit launched in 1994, launched a prize around private spaceflight, which expedited breakthroughs and helped foster the industry: XPrize Fondation (last accessed Sept. 3, 2020), https://www.xprize.org/home; The Bill and Melinda Gates Foundation hosts a Grand Challenges in Global Health program that focuses on key scientific challenges that could lead to advances in preventing, treating, and curing diseases of the developing world. See *About Grand Challenges*, Bill and Melinda Gates Foundation (last accessed Sept. 3, 2020), https://gcgh.grandchallenges.org/about; see current U.S. government funded challenges at Challenge.gov (last accessed Sept. 3, 2020), https://www.challenge.gov/.

[51] See Vanessa Pena & Chelsea A. Stokes, *Use of Grand Challenges in the Federal Government*, IDA Science & Technology Policy Institute (June 2019), https://www.ida.org/-/media/feature/publications/u/us/use-of-grand-challenges-in-the-federal-government/d10699final.ashx. Not all challenges are prize-based. For example, the National Nanotechnology Initiative launched a challenge in 2015 to focus the research community and government funding agencies to advance the future of computing by harnessing nanotechnologies. See *A Nanotechnology-Inspired Grand Challenge for Future Computing*, Nano.gov (Oct. 20, 2015), https://www.nano.gov/futurecomputing

[52] See Vanessa Pena & Chelsea A. Stoke, *Use of Grand Challenges in the Federal Government*, IDA Science & Technology (June 2019), https://www.ida.org/-/media/feature/publications/u/us/use-of-grand-challenges-in-the-federal-government/d10699final.ashx

[53] See *The DARPA Grand Challenge 10 Years Later*, DARPA (Mar. 13, 2014), https://www.darpa.mil/news-events/2014-03-13.

[54] As DARPA did through the Spectrum Challenge and the currently-running subterranean challenge. See *Spectrum Collaboration Challenge*, DARPA (last accessed Oct. 13, 2020), https://archive.darpa.mil/sc2; Unearthing the Subterranean Environment, DARPA (last accessed Oct. 13, 2020), https://www.subtchallenge.com/#top. For discussion of the power of challenges to drive AI research, see Yolanda Gil & Bart Selman, *A 20-Year Community Roadmap for AI Research in the US*, Computing Community Consortium and Association for the Advancement of Artificial Intelligence (Aug. 6, 2019), https://cra.org/ccc/wp-content/uploads/sites/2/2019/08/Community-Roadmap-for-AI-Research.pdf.

The challenge should be designed to spark breakthrough advances in one or more areas including but not limited to:

- **Human-robotics teaming and human-AI collaboration**. Effective, complex cooperation between humans and machines in open, unknown, and dynamically changing environments, including high-stakes situations that put people under cognitive load and time pressure.

- **Convergence of AI capabilities**. Integrating a system of systems that benefits from leveraging different types of AI technologies and capabilities, including language abilities, machine vision (e.g., for scene understanding), planning, transfer learning and generalization, and more.

- **Leap in language understanding**. Language understanding that can enable grounded, collaborative conversations and transfer of knowledge between a human and machine through spoken or written language.

- **Real-time forecasting and development of intervention options**. Continual modeling and generation of analysis and action plans in response to dynamically evolving events, for example, natural disasters such as hurricanes, floods, and fires.

- **Self-aware learning**. Incorporation of commonsense reasoning, logic, and domain knowledge, such as physics or biology, into learning, while quantifying uncertainty. Learning in an unsupervised manner from data in the wild and generalizing prior learning.

For maximum effect, the challenge should:

- Have AI at its core.

- Develop technology towards a greater public good.

- Embody an ambitious goal that can be broken down into a series of more discrete problems that—together with clear metrics to measure progress—create a long-term research arch.

- Hold relevance to future national security capabilities.

- Allow for creativity in use of a diversity of AI approaches.

- Be designed in a way that negates the ability of participants to "game" the competitions or to employ shallow problem-solving methods.

- Create shared resources to support the competition—including data sets, tools, and testbeds; and be configurable for "digital twin" and simulated components.

- Partner with relevant interagency organizations that maintain domain and operational expertise.

- Pair with planned and budgeted multi-year funding to support further development of resulting technological advancements.

The Commission recommends an expert panel is convened to build a challenge that satisfies the above-mentioned goals. To give a sense of the scale, style and level of inspiration required, we provide the following example:

Enabling Effective Natural Disaster Response

Hurricanes, for example, are a persistent threat. AI could help America plan and prepare for, and respond to these and other natural disasters in myriad ways–ranging from helping build response plans, further increasing the accuracy of two-day, one-day and eight-hour forecasting, maintaining situational awareness during a storm, expediting command and control in the 12 hours after a storm, detecting people for search and rescue operations, optimizing logistics in the seven days after the storm and for longer term recovery efforts.[55] Each of these represent areas where the country already holds considerable expertise, but each also represents an opportunity ripe to exploit AI advancements from the past three to five years and to inspire new advancements in AI technologies.

For a challenge, one could imagine a program to obtain and assimilate many forms of aerial and spaceborne imagery obtained during the first 24 hours after a storm (visible, infrared, lidar, radar) to build, display, and summarize the full operational picture in a way that could transform shared planning, triaging of rescue missions, real-time evacuations, and near term infrastructure risks. This could include use of in-situ, crowd sourced, and non-traditional datasets to inform and drive post-landfall response operations in real time.

This project would embody an ambitious goal that would capture public imagination; require expertise in computer vision, active learning, sensor fusion from multiple modalities, machine learning, model-based planning and thorough design of how computers can best advise humans who are being overwhelmed with information. Furthermore, aspects of the challenge could be objectively judged based on data from previous storms and others by simulation.

Recommended Legislative Action

The Commission recommends that Congress appropriate an additional $75 million to DARPA's budget in order to support the launch of an AI grand challenge.[56]

[55] Indeed, creation of a digital twin testbed for the challenge would also facilitate running "exercises" to prepare multiple contingency plans and prepare in a high fidelity environment.

[56] This would support around 10 teams for the length of the five year challenge. With additional funds to provide for incentive prizes to meet benchmark problems within the challenge framework and support establishment of infrastructure and shared resources.

Issue 2: Creating a Digital Ecosystem for National Security AI R&D

For U.S. national security and defense to realize a future that incorporates AI-driven capabilities at scale and speed, it is essential to build a digital AI R&D[57] ecosystem that serves the DoD, Intelligence Community (IC), and DoE, bringing together critically necessary infrastructure, resources, and services. Just as the Commission recommended creation of an AI Research Resource to democratize access to compute and data to fuel AI R&D in the open research environment,[58] the United States Government must equip researchers and developers within the national security community with the services, tools, and environments necessary to accelerate innovation in AI.

As NSCAI's *2019 Interim Report* highlighted, much of the United States Government's data is unlabeled and hidden in various silos across disparate agencies and networks. But sharing data is just the first step. For example, in the Commission's *Second Quarter Recommendations*, the Commission recommended actions to accelerate AI R&D across the DoD research enterprise, to include creating an AI software repository and advancing TEVV capabilities.[59] Building on such local resources, an interagency digital AI R&D ecosystem should embody a networked architecture[60] supporting a diversity of AI approaches[61] that connects researchers and developers to federated repositories hosting data,[62] trained AI models, and AI software tools made accessible through user-based authentication;[63] along with AI testbeds and test ranges; and distributed computing resources and support.[64] Such a construct would provide widespread benefit to agency missions by reducing duplicative efforts, leveraging scarce technical talent, improving the performance of algorithms, and increasing the speed at which capabilities are fielded.

[57] The definition of AI R&D to be supported by the digital ecosystem is intended to be broad—spanning DoD research budget activity categories (6.1 through 6.7) as well as research outside appropriations categories.

[58] *First Quarter Recommendations*, NSCAI at 12 (Mar. 2020), https://www.nscai.gov/reports.

[59] See *Second Quarter Recommendations*, NSCAI at 2-15 (July 2020), https://www.nscai.gov/reports (Issue #1: Equipping the Enterprise for AI R&D and Issue #2: Establishing AI Test, Evaluation and Verification and Validation Capabilities).

[60] Such a network architecture may in itself be federated, integrating with other efforts underway such as with the DoD's Joint Information Environment (JIE) Framework. "The JIE Framework also provides a networking design that improves defenses against malicious cyberspace activity and is managed through a tiered structure of network operations and security centers." *DoD Digital Modernization Strategy*, U.S. Department of Defense at 7 (July 12, 2019), https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF. [hereinafter, *DDMS*]

[61] Including but not limited to expert systems, model-based AI, statistical machine learning, and future AI approaches (e.g., what DARPA calls third wave AI).

[62] This includes types of data across the data lifecycle including raw, curated, and training data sets.

[63] See *DDMS* at 30 and 42-43 (describing how the DoD plans to deploy an end-to-end identity, credential, and access management infrastructure). This is an essential function that must be implemented in an interoperable way across the national security-wide digital AI R&D ecosystem. DoD plans include "Strategy Element #7: Improve and Enable Authentication to DoD Networks and Resources through Common Standards, Shared Services, and Federation." Id. at 30.

[64] See *DDMS* at 14. This digital ecosystem is in alignment with the DoD Digital Modernization Strategy which envisions "a rich and diverse set of analytic capabilities fueled by data from sensors across the DoD Information Network (DODIN). Modernization of the Defense Information Systems Network, a key component of the DODIN, will provide critical enhancements necessary to fully realize the benefits from cloud computing, big data analytics, mobility, Internet of Things, increased automation and cognitive computing." Id.

This vision represents a foundational layer for the U.S. national security sector to develop AI at scale. Operational deployment of AI solutions and systems will leverage and reflect many components of this construct, with additional requirements pertaining to specificities of battle networks, systems, and agency missions. The Commission continues to develop a vision of the key elements and investments that will enable operational deployment of AI at speed and scale.

Today, portions of necessary resources and services for AI R&D exist in individual agencies at various levels of maturity.[65] But, while each agency is investing to overcome technical debt, these investments are often redundant, uncoordinated, and not integrated to create a platform of shared resources necessary for scaling and accelerating development of AI for national security capabilities.

Implementation should build on a minimal level of utility and evolve into an extensible and scalable architecture that embraces future advancements in AI and infrastructure technologies.[66] This incremental approach allows for new AI resources and services to be developed and deployed bottom-up from within agencies, tuned to meet local mission needs. Top-down coordination will then set the conditions for responsible sharing of these resources across the national security enterprise. This would lower the barrier of entry and fuel a virtuous cycle of innovation that harnesses the collective expertise of the national security technical community and leverages leading commercial capabilities.[67]

At its core, the approach should be service-oriented—tying together independently emerging resources across national security agencies into a holistic architecture[68] that is discoverable through a distributed registry system[69] and shareable through common service interfaces and linked repositories. Embodying the adage, "the whole is greater than the sum of its parts."

Such a digital ecosystem should be based on the following guiding characteristics:

1. **Federated.** Linking together a dynamically evolving set of dispersed, shared resources, accessible through common, controlled, and authorized interfaces.[70]

[65] For example, the DoD's Joint Artificial Intelligence Center (JAIC) is establishing these within its Joint Common Foundation to provide baseline tools and services to serve its internal efforts.

[66] For example, the eventual operationalization of quantum computing and quantum communications.

[67] Evolving the digital ecosystem in this fashion is in alignment with the DoD Digital Modernization Strategy approach that "will enable continual, comprehensive Department-wide IT modernization in a common, coordinated way. Furthermore, it will accelerate transition to foundational enterprise capabilities and services . . . ." DDMS at 12.

[68] The ecosystem should be architected to appropriately support AI R&D at all levels of security classification.

[69] Similar to or relying upon the platform delivery and features of Git (https://git-scm.com), GitHub (https://github.com), and GitLab (https://about.gitlab.com). According to the DoD's digital modernization strategy, "essential infrastructure (e.g., IT services registry, meta data registry, authoritative data source registry) and defined, standardized data tags or labels do not currently exist. Additionally, the Department has no enterprise search capability to enable discovery of critical DoD data across its network security domains." DDMS at 17.

[70] This would build a scalable enterprise-wide AI R&D ecosystem by tying together a growing network of evolving local but shared resources, avoiding the approach of a monolithic (one-size-fits-all) solution.

2. **Service-oriented.** Offered services[71] and resources that are discoverable and queryable, with access tied to user-specific authorization and authentication.[72]

3. **Governed.** Clear policies, practices, and supporting technical structures and mechanisms to ensure compliance with access, classification level, and privacy and civil liberty controls[73]—mitigating security risks and incentivizing a culture of responsible openness.[74]

4. **Scalable & Extensible.** Scaled in a manner that expands on pathfinder efforts, increasing over time the number of deployed and evolving resources and services—propagating lessons learned and (where appropriate) documentation and/or code.[75]

5. **Automated.** Administration automated to the maximum extent possible,[76] minimizing human involvement in vetting compliance, classification, and access, while maintaining human oversight and accountability.[77]

6. **Innovative.** Able to nimbly leverage new ideas and solutions coming from the private sector—not only from leading technology companies, but also from non-technology sectors pioneering AI infrastructure solutions;[78] and integrate contributions from small businesses and academia at the granular level of capabilities and microservices.

[71] This refers to "digital" services providing access to data, trained AI models, software, and computing. Not in scope are "human" services such as help desks and application support.

[72] Such an approach would provide access to AI R&D resources using a uniform service-oriented approach that supports independent implementations of local but shared resources. Offered services must be discoverable to outside researchers and developers (a.k.a., users) in a controlled manner, so that only those with the proper level of authorization can inquire and see the "exposed" services. Users must be able to query an exposed service in a uniform way to sufficiently understand how to engage with it.

[73] In our *Second Quarter Recommendations*, the Commission recommended practices to help ensure that AI systems and their uses align with U.S. values and the rule of law. See *Key Considerations for Responsible Development & Fielding of Artificial Intelligence*, NSCAI at 7-14 (July 2020), https://www.nscai.gov/reports. [hereinafter Key Considerations]

[74] There are many areas of policy in need of further development, for example, attributing algorithmic accountability, requiring algorithmic explainability, and establishing clear practices to ensure compliance with acceptable uses for certain data sets. Mechanisms to establish policy compliance are needed to appropriately vet and match users with use, and with the requested service including classification and security levels, privacy controls, controlled authorized access, and cybersecurity. The ecosystem requires a thorough and systematic approach to establish incentives for all stakeholders, creating a culture for success. Local resource hosts, internal users, as well as external users must derive value from resource sharing.

[75] This can be realized with an elastic cloud infrastructure that can expand and contract storage and computing resources as needed.

[76] Areas of automation include: identity management and the access rights; data rights and licensing; software rights and licensing; research protocols and protections (e.g., personally identifiable information and protected health information); declarations of ethical and responsible use; access and migration across the levels of network security; and uniform service interfaces.

[77] See Key Considerations at 32-35 (recommending practices to help ensure optimal human-AI interaction) and at 35-37 (recommending practices to help ensure accountability and governance for an AI system's inferences, recommendations, and actions, as well for its maintenance and auditing).

[78] For example, commercial retail, logistics and delivery, and advanced manufacturing.

A framework for implementation should marry top-down strategic coordination and direction with bottom-up distributed mission implementation to realize a national security-wide digital ecosystem in a manner that will not slow innovation, but rather incorporate new capabilities at the speed of innovation and mission requirements. This will require development of a coordination and implementation roadmap informed by internal stakeholders, external experts, and overseen by senior leadership.

Funding must support resource sharing outside the host's internal community of users, and success will require a long-term commitment to support infrastructure investments including timely recapitalization and/or expansion.[79] Further, success will rest on effective policy and practice for resource allocation to ensure that a host's internal user needs are met, while metering the resources that are shared with external users.

The following components represent the foundational pillars of the ecosystem:

- **Data.** The ecosystem's federation of data repositories[80] linked across the DoD, IC, and DoE should serve both data sets and associated data models.[81] Data must be sufficiently documented,[82] traceable,[83] and composable;[84] and secured with controlled access by authorized users.[85] There should also be support for synthetic data generation and data augmentation.[86] The goal of these data resources is to provide a growing number of AI-ready data sets to empower communities of researchers across the national security enterprise to use AI to advance research, science, and mission capabilities in strategic areas.[87]

[79] Using sponsored program funding to build resources, by policy, restricts the use of the resulting resources to the users of the program. Centralized funds expressly for shared resources can avoid such limitations.

[80] There are many types of data that can be collected and sampled in ways tailored to specific use cases resulting in growing repositories of different data sets. A data set should be strategically reused only when these characteristics are known to be appropriate for the new R&D effort.

[81] Sharing of data models (e.g., data set schema) is essential for interoperability and joining with other data sets. Under some circumstances it may be possible and helpful to share a data set's model even if the data itself cannot be shared.

[82] The application of data documentation and annotation standards are required. See *First Quarter Recommendations*, NSCAI at 71 (Mar. 2020) (Issue #2: Documentation on Data, Models, and Systems).

[83] Traceable at the smallest logical units of data across the data management lifecycle. This function will likely not be achievable at the ecosystem's initial minimal level of utility, but this should be added as quickly as technically possible looking to industry for viable solutions.

[84] The ability to compose training and testing data sets by selecting and joining together data from multiple sources relies on sufficient documentation to do so in a responsible, ethical, and compliant manner. See Key Considerations at 18-20; 22 (noting urgency of a documentation strategy and describing minimum data documentation requirements) and at 19 (recommending infrastructure to support traceability).

[85] The ecosystem must employ modern tools to enhance both the sharing and the safeguarding of these resources, and there is need for a uniform policy and practice for managing authoritative, shared user attributes to control who will build, use, or share these AI resources accounting for national security classification levels.

[86] Guidance should be included for when to use, and when not to use, these capabilities. Special care must be taken to convey the limitations and intended uses of synthetically generated data and other data augmentation methods.

[87] See *DDMS* at 17-18 (describes how the DoD plans to treat data as a strategic asset, including "Strategy Element #2: Invest In and Maintain the Infrastructure Required to Make DoD's Data Visible, Accessible, Understandable, Trusted, and Interoperable") and at 22 (for a data use case example, "Strategy Element #1: Establish Capabilities to Support Ingest, Accumulation, and Global Delivery of [End-to-End Airborne Intelligence, Surveillance, and Reconnaissance] AISR Data from Multiple Platforms/Sources").

- **Trained AI Models.** Models contain compact information derived, for example, from vast amounts of data, expert knowledge, or physics parameters to support automated decisions or actions.[88] By sharing trained AI models, the rich, compact information can be reused with little additional computational cost for fine-tuning and/or making decisions on new data streams. In some cases, sharing a trained AI model may be possible even when the training data itself may be sensitive and cannot be shared.[89] Resourcing sharing of pre-trained AI models[90] requires each model to be sufficiently documented, authenticated, as well as appropriately secured and access controlled.[91]

- **AI Software Tools.** Sharing of software, be it open source, United States Government procured,[92] or internally developed should be enabled through federated, portable, interoperable and observable repositories.[93] The shared sets of software tools must have Authority to Operate reciprocity[94] built in and be sufficiently documented.[95]

[88] The information content, and what is represented, changes depending on the AI approach being used. Note this federated repository of trained AI models is not to be limited to those created by statistical machine learning, but to the extent possible be agnostic to the AI approach used, and also include models based on expert knowledge, models based on physics knowledge, and AI approaches of the future. The future will likely be defined as a fusion of these varied approaches.

[89] This is possible due to the transformation of data into a different compact informational representation. Note it has been shown that training data can be reconstructed to some level of fidelity through purposeful interrogation of the model. To ensure zero chance of model "leakage" requires the use of privacy preserving machine learning techniques that are still a topic of research. Therefore, sharing of trained AI models today must be based on trust and risk assessment.

[90] These are not homogenous nor universal and would reflect a wide variety of use cases. Sharing and reusing AI models must account for differences based on the data used in training, the purpose for which the model was trained, and the AI approach and configuration settings used. Models should only be applied on new data streams that are deemed compatible with how the model was trained in order to ensure the model operates as expected. This information must be meaningfully conveyed to end users to ensure models are applied appropriately.

[91] A new policy and practice for documenting trained AI models is required in order to support issues including: the model's provenance for credibility and authenticity; the ethical and responsible use of the model in new operational contexts (e.g., knowing the model's designed purpose, limitations, and restrictions); and the appropriate augmentation of the model (e.g., additional training to tune the model to a new operational context). See Key Considerations at 18-20; 22 (recommending that model documentation include the intended uses of the AI capabilities separately or as part of another system, and recommending that documentation include re-testing, retraining and tuning requirements for a system that is used in a different scenario or setting than originally intended) and at 20-21 (recommending practices to address adversarial attacks and unintentional failures and the adoption of a security development lifecycle for AI to address potential failure modes).

[92] Note that the extent to which government procured AI software is shared will depend on the terms of the software's license agreement.

[93] These shared tools will be able to be updated via their repositories in order to address any bugs or security vulnerabilities that are later discovered. End users of the shared software tools should adopt best practices to ensure they are using the most up-to-date versions of the codebase.

[94] Software ATO reciprocity is critical to achieving the agility, speed, and automation needed to support DevSecOps. Adding sufficient documentation in the body of evidence for ATO might accelerate reciprocity, as well as inviting other organizations to be part of a joint security testing team and/or multi-party red team. In our *Second Quarter Recommendations*, the Commission recommended promotion of ATO reciprocity as the default practice within and among programs, Services, and other DoD agencies to enable sharing of software platforms, components, infrastructure, and data for rapid deployment of new capabilities. See *Second Quarter Recommendations*, NSCAI at 5 (Issue 1: Recommendation 2); see also DDMS at 32 (reinforces the need to "Strategy Element #5: Expand the Use of Proven Software and Hardware Assurance Methods").

[95] Software documentation to include source, licensing, authorizations, and other metadata to support compliant usage. Examples of tool sets include: data lifecycle management, AI development pipeline (e.g., supporting

- **TEVV Services.** A growing variety of TEVV services[96] including local software-based testbeds supported by downloadable TEVV software stacks as well as large persistent AI test ranges that support live, virtual, or blended environments, should be established to support the diversity of AI applications and ensure responsible fielding of AI systems.[97] All these TEVV services should be based on a flexible, evolving, and common testing framework.[98]

- **Computing Resources and Support.** Diverse and distributed computing resources should support a range of requirements across the ecosystem.[99] For example, at times data can be moved to the researcher's computing environment; and at other times due to the size or sensitivity of the data,[100] the researcher's analytic must be moved to where the data is hosted for the computation to take place there. Policy and practice will need to be developed in order to responsibly and proactively manage the load and priorities of these shared computing resources to avoid resource contentions.

These pillars must be woven into the network architecture of the digital ecosystem through a uniform layer of shared services based on common interfaces that make these essential resources discoverable, usable, deployable and maintainable. This will pay widespread dividends by reducing duplicative efforts, which will free up scarce technical talent to apply AI to mission needs,[101] which will, in turn, lead to improved performance of algorithms and increased speed at which capabilities are fielded.

DevSecOps), TEVV (e.g., ethical and responsible AI evaluation including tools to detect and mitigate unintended bias), machine learning and data analysis, AI red teaming, AI modeling and simulation, synthetic data generation and data augmentation, and AI software stacks and platforms (including autonomy and edge AI). See Key Considerations at 21-22 (recommending that red teaming be conducted for both intentional and unintentional failure modalities).

[96] As stated in the NSCAI *Second Quarter Recommendations* - Issue 2: Recommendation 6, "Expedite the development of tools to create tailored AI test beds supported by both virtual and blended environments," on 14.

[97] The Test Resource Management Center's roadmap for delivering an enterprise-level Joint Autonomy & Artificial Intelligence Mobile Test Harness/Range is a prime example of such a test range. Note that these types of test environments are also useful in developing AI capabilities, for example when applying reinforcement learning.

[98] See NSCAI *Second Quarter Recommendations*, NSCAI at 12 (July 2020) (Issue 2: Recommendation 5, "Establish an AI testing framework"); *Key Considerations* at 25-29 (recommending specific training and testing practices, including standards for metrics and reporting to achieve consistency and iterative testing, for instance). These TEVV services are intended to improve the consistency and quality of AI technology performance assurance. Best practices should be developed and adopted to enable testing reciprocity so that testing that takes place within one component is recognized and accepted by another. This would remove unnecessary redundancies and accelerate the process of AI-driven capability development to deployment.

[99] This spans support for cloud computing, high performance computing, edge computing, and embedded computing in autonomous platforms. See DDMS at 15-16 (Describes how the DoD plans to deliver a DoD enterprise cloud environment to leverage commercial innovation. Of particular note are "Strategy Element #2: Identify Common Niche Capabilities to Inform the Creation of Fit for Purpose (F2P) Cloud Environments Practices" and "Strategy Element #7: Develop and Deploy a DevSecOps Environment that Enables Application Development and Accreditation at Speed and Scale Integrated with Defensive Cyberspace Operations") and at 25 (While cloud-based resources are encouraged, it is important to note that not all computing environments will be cloud-based. For example, the DoD includes "Strategy Element #1: Migrate DoD Applications and Systems that Cannot be Hosted in Commercial Cloud Environments to Enterprise Data Centers").

[100] The network bandwidth and security classification level also factor into these limitations.

[101] See *DDMS* at 12 (the benefits and efficiencies to this type of approach are called out).

Issue 3: Expanding Industry's Role in DoD's AI R&D to Develop Next-Generation Capabilities

American companies are at the forefront of AI research and development. Their cumulative investments dwarf federal R&D[102] and attract top global talent. The paradigm of the 20th century was government-sponsored technology breakthroughs, the exemplars of which were the Manhattan Project and the Internet. In the 21st century, the private sector, endowed with an unprecedented concentration of wealth in the digital age, has led the way. The DoD's responsibility in this new era is to find novel and effective ways to integrate commercial technology, fund basic research, and incentivize pre-commercial investments.

The Department has a long history of working with industry on R&D, a partnership that helped win the Cold War. The model was predicated on the government as both the primary investor and the largest buyer of final goods. Today, the demands of global consumers drive industry investments in R&D at a scale that government grants and contracts cannot match. Shareholder demand for quarterly reporting rewards incremental improvements over competitors. The anti-government sentiment among technologists in the aftermath of the Edward Snowden leaks has moderated but continues to limit direct partnership with certain firms. At the same time, the reemergence of great power competition and the military-technology challenge posed by China make partnering with the tech sector more important than ever.

The scale of government funding can still influence the research priorities and viability of early-stage startups, which often succeed or fail in the first year. This makes small technology companies an important partner for AI R&D that can build future defense and national security capabilities. Recognizing this opportunity, the Central Intelligence Agency (CIA) founded In-Q-Tel in 1999 as a non-profit organization to "ensure that the CIA remains at the cutting edge of information technology"[103] through equity investments, product development funding, and warrants.

The Department of Defense began tackling the issue in 2012, and over the course of several years, launched multiple initiatives to bridge the gap with Silicon Valley and support the military transfer and application of cutting-edge technology[104]: the Defense Innovation Board (DIB), Strategic Capability Office (SCO), Defense Innovation Unit (DIU), and Defense Digital Services, among others. The Services and Combatant Commands introduced pathfinder organizations—AFWERX, SOFWERX, NavalX, Kessel Run, Platform One, Army Futures Command—towards a similar goal.

[102] U.S. firms Alphabet, IBM, Facebook, Microsoft, and Amazon spent an estimated $80.5 billion on AI R&D in 2018. Unclassified federal expenditure on defense AI R&D is estimated at $4 billion in fiscal year 2020. Non-defense AI R&D is closer to $1 billion. See Martijn Rasser, et al, *The American AI Century: A Blueprint for Action*, CNAS (Dec. 17, 2019), https://www.cnas.org/publications/reports/the-american-ai-century-a-blueprint-for-action; Chris Cornillie, *Finding Artificial Intelligence Money in the Fiscal 2020 Budget*, Bloomberg Government (Mar. 28, 2019), https://about.bgov.com/news/finding-artificial-intelligence-money-fiscal-2020-budget/.

[103] *In-Q-It, CIA Partner to Find Leading-Edge Technology Solutions*, Central Intelligence Agency (Sept. 29, 1999), https://www.cia.gov/news-information/press-releases-statements/press-release-archive-1999/pr093099.html.

[104] *Annual Report 2019*, Defense Innovation Unit (2019), https://assets.ctfassets.net/3nanhbfkr0pc/ZF9fhsMe6jtX15APMLalI/cd088a59b91857c5146676e879a615bd/DIU_2019_Annual_Report.pdf.

These organizations have made significant progress in improving access to nontraditional contractors and scouting commercial technology. DIU leverages Other Transaction Authority[105] (OTA) and the Commercial Solutions Opening process to "test, field, and scale commercial technology in less than 24 months."[106] The Army Applications Laboratory (AAL) works with Army Futures Command to bring the Force's most pressing technology problems to private-sector innovators.[107] The Air Force's AFWERX, in partnership with Air Force Research Lab (AFRL) and DIU's National Security Innovation Network (NSIN), has pioneered new approaches to Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) funding to "increase the efficiency, effectiveness, and transition rate" of the program.[108] They have also introduced challenges and competitions, following the precedent set by DARPA and Hacking for Defense, to bring together the defense, academic, startup, and private sector communities around priority problems.

Other pathfinder organizations focus on creating unique ecosystems within the Department that physically and culturally emulate Silicon Valley. The Air Force's in-house software factories[109] and its DevSecOps Enterprise Services team Platform One "have managed to entice coders with Silicon Valley-style office cultures and remote work options."[110] Naval X introduces "non-traditional agility methods," including best practices in software development, to the Navy's own workforce.[111] Its Tech Bridge program provides off-base, commercial business spaces to "enhance[] collaboration between Naval Labs, industry, academia, and other military branches" across the country.[112]

The co-location of researchers and end-users, facility clearance and access to secure data, among other conditions, aims to create an environment that encourages experimentation, breaks down red-tape and bureaucratic hurdles, and attracts top talent. Such models have been successfully leveraged by the Army's A4I Innovation Framework—a collaboration between Carnegie Mellon University and the Army Futures Command—and the Massachusetts Institute of Technology-Air Force Accelerator. Both efforts lower physical and digital barriers between academia and the Services by leveraging Federally Funded Research and Development Centers as bridges.

Pockets of successful bottom-up innovation, while promising, cannot translate into strategic change without top-down leadership to synchronize efforts and overcome organizational

[105] Congress amended the OTA to provide the DoD with "authority . . to carry out certain prototype projects" in the National Defense Authorization Act for Fiscal Year 2016. Pub. L. 114-92, div. A, title VIII, §815(a)(1), 114th Cong. (2015), 129 Stat. 893. [hereinafter OTA]

[106] *Annual Report 2019*, Defense Innovation Unit (2019), https://assets.ctfassets.net/3nanhbfkr0pc/ZF9fhsMe6jtX15APMLalI/cd088a59b91857c5146676e879a615bd/DIU_2019_Annual_Report.pdf.

[107] A*rmy Applications Laboratory*, U.S. Army (last accessed Sept. 15, 2020), https://aal.army/.

[108] *SBIR Open Topics*, U.S. Air Force AFWERX (last accessed Sept. 15, 2020), https://www.afwerx.af.mil/sbir.html.

[109] Kessel Run, for example, was incubated by DIU and now has its own DevOps lab—the Kessel Run Experimental Laboratory. For more see *Kessel Run*, U.S. Air Force (last accessed Sept. 27, 2019), https://kesselrun.af.mil/. For a full list of Air Force software factories see *Software Factorie*s, U.S. Air Force (last accessed Sept. 27, 2019), https://software.af.mil/software-factories/.

[110] *New Air Force deputy CIO says her dedication to IT 'foundation' won't change*, Fedscoop, September 8, 2020, https://www.fedscoop.com/lauren-knausenberger-billington-cyber-interview/.

[111] *Welcome To NavalX*, U.S. Navy NavalX, (last accessed Sept. 15, 2020), https://www.secnav.navy.mil/agility/Pages/default.aspx.

[112] *Tech Bridges*, U.S. Navy NavalX, (last accessed Sept. 15, 2020), https://www.secnav.navy.mil/agility/Pages/techbridges.aspx.

barriers.[113] Pathfinder organizations continue to face challenges transitioning viable advances from prototypes to programs of record. In some cases, requirements-based contracts and research grants incentivize the delivery of bespoke products never designed to scale. In other cases, prototypes are doomed from the outset because companies are not provided the institutional or technical support to succeed. The Department collaborates well with academic and non-profit institutions but continues to treat the private sector as primarily a marketplace for finished goods, not a potential partner in innovation.

This dynamic, along with the complexity and duration of the DoD procurement process, discourages non-traditional companies and investors from entering the defense sector. Bridging and innovation organizations have made impressive progress on communication with the commercial sector, but signaling of defense priorities and future opportunities that can inform private investments remains scattershot. For emerging technologies like AI, where expertise and resources overwhelmingly reside in the private sector, the national security community cannot afford to maintain this posture.

The Department needs to define a strategy for partnering with the private sector on AI R&D that optimizes for its comparative advantage and prioritizes based on need and mission set. This means taking advantage of existing solutions in areas where the private sector excels, and leading in areas of AI R&D overlooked by the private sector that may have important national security applications. It also means allocating resources discriminatively: identifying where significant federal investments are necessary, versus where small investments or policy changes "nudge" industry towards technologies with future defense applications.

Furthermore, this strategy must be communicated externally, to where the bulk of the AI talent resides. Shifting to a more integrated and transparent communication of priorities would enable Defense primes and non-traditionals to plan and invest more to help meet DoD R&D needs. Expanding technical exchanges between DoD and the private sector would also help firms plan their R&D investments, encouraging the growing number of startups focused on solving national security problems.

Recommendation 6: Communicate DoD Modernization Priorities to Industry through Issuance of Technology R&D Objectives

NSCAI's *Interim Report* called for the United States Government to "identify, prioritize, coordinate and urgently implement national security-focused AI R&D investments."[114] This initial assessment has been reiterated across the Commission's engagements with the private sector. Defense primes, non-traditional contractors, and investors all call for greater transparency around the DoD's AI priorities, so that they can better direct internal resources. In the venture capital world, there exists interest and available capital for defense-specific and dual-use technologies, but investors need to know that there will be a federal market for the product.[115] SBIRs have become one form of informal signaling, but the scale of postings and active contracts obfuscates prioritization.[116]

[113] See *Interim Report*, NSCAI at 31 (Nov. 2019), https://www.nscai.gov/reports.
[114] Id. at 27.
[115] NSCAI staff engagement (Aug. 11, 2020).
[116] There are over 200 available funding topics for DoD SBIRs. See *DoD 2020.1 SBIR Solicitation*, DoD SBIR STTR (Dec. 10, 2019), https://www.sbir.gov/node/1654283.

In pursuing its mandate to address novel, technology-related threats, set technical direction, and drive the DoD investment strategy, the Office of the Undersecretary of Defense for Research and Engineering (OUSD(R&E)) has issued R&D priorities for the Department through technology focus areas, referred to as "modernization priorities."[117] The current list comprises: AI; Biotechnology; Autonomy; Cyber; Directed Energy; Fully Networked Command, Control, and Communications Technology; Microelectronics; Quantum Computers; Hypersonic Weapons; Space; and 5G.[118]

For each modernization priority, a principal director has been appointed to oversee investments and capabilities, and build a road map to "integrate and evaluate" ongoing activities and provide guidance on future directions.[119] However, while these categories[120] are helpful as a strategic tool to harness the energies of the defense research enterprise and broadly signal to the private sector, they are limited in how effectively they can steer commercial R&D towards efforts that parallel DoD's key technology interest areas. Modernization priority road maps should include definitions of subsets of the technology focus area in question that OUSD(R&E) assesses to be a priority or a gap that industry R&D could help advance.

Furthermore, in line with the reconstituted and expanded technology scouting role envisioned for OUSD(R&E) in Tab 2 of this memo, OUSD(R&E) should be tasked to publicly publish R&D objectives to support existing modernization priority roadmaps and the Technology Annex to the National Defense Strategy.[121] The R&D objectives should be tied to subsets or components of the modernization priorities on which the government envisions the private sector playing a major role in building future capabilities. For example, under microelectronics this might include advancing AI multi-chip packages, development of quantifiable assurance, 3D chip stacking, photonics, carbon nanotubes, Gallium Nitride transistors, domain-specific hardware architecture, electronic design automation, and cryogenic computing.[122]

These commercially-oriented resources should be living documents, regularly updated in accordance with evolutions in technology and strategic defense priorities, with associated communications plans that can inform and assist the work of stakeholders such as DIU,

[117] For a full list of USD(R&E)'s responsibilities and functions, see *DoD Directive 5137.02*, DoD (July 15, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/513702p.pdf?ver=2020-07-15-124712-047.

[118] Section 255 of the National Defense Authorization Act for Fiscal Year 2020 directed USD(R&E) to develop a National Defense Science & Technology Strategy. Pub. L. 116-92, sec. 255, 116th Cong. (2019); see also *Modernization Priorities*, DoD USD R&E (last accessed September 7, 2020), https://www.cto.mil/modernization-priorities/.

[119] Melissa Harris, *How DOD's Modernization Approach is Shifting Top Tech Priorities*, Government CIO Media (May 19, 2020), https://governmentciomedia.com/how-dods-modernization-approach-shifting-top-tech-priorities (quoting DoD's Research and Engineering for Modernization Director Mark Lewis). Reporting indicates that USD(R&E) has completed roadmaps for some modernization priorities such as hypersonics and is working on or nearing completion on others such as microelectronics. See Jon Harper, *Pentagon Reshuffles R&D Priorities*, National Defense (Jun. 6, 2020), https://www.nationaldefensemagazine.org/articles/2020/6/5/pentagon-reshuffles-rd-priorities.

[120] The description for AI is as follows: "The DoD will leverage AI to enable U.S. forces to operate more effectively and efficiently. As a Department, we are evaluating which of our processes and procedures can be enabled via adoption of AI technology to meet warfighter needs and Defense priorities."

[121] An interagency technology scouting community of practice, as well as the enterprise AI-powered analytic resources envisioned in Tab 2, would inform the R&D objectives and assist USD(R&E) in better understanding current investments, future capabilities, and commercial technology trajectories.

[122] As recommended by NSCAI in our *First Quarter Recommendations*.

AFWERX, and NavalX. They must strike the delicate balance of effectively communicating enough detail to clearly signal to future industry partners, without betraying sensitive priorities or weaknesses to adversaries.

Critically, in order to execute this task, OUSD(R&E) must be staffed with personnel that have the technical expertise and commercial proficiency to communicate these capabilities in terms that industry can understand and act upon. The Commission's *First Quarter Recommendations* called out the need for departments and agencies to "increase the number of fellowships and partnerships with industry, particularly fellowships with AI and software companies."[123] OUSD(R&E) should take advantage of public-private exchange programs, as well as internal technical expertise from entities like DARPA, to bring the right talent to the effort.[124]

If managed effectively, communication of these R&D objectives would provide current defense companies guidance to steer their internal R&D investments, communicate to startups interested in working with the government where future opportunities lie, and signal to venture capitalists where future DoD funding might flow.

Proposed Executive Branch Action

The Commission recommends the Secretary of Defense task OUSD(R&E) to produce unclassified emerging technology R&D objectives to be released regularly to the commercial sector and aligned with subsets of technology underneath the modernization priorities.

Recommendation 7: Strengthen Return on SBIR Investments

The SBIR program is one of the largest and longest standing programs for federally funded R&D in small businesses. Established in 1982 as part of the Small Business Innovation Development Act, Federal agencies with extramural research and development budgets that exceed $100 million set aside 3.2 percent of their budgets to fund the SBIR program. The program is structured in three phases: Phase I awards of approximately $50,000 - $250,000[125] for six months to vet "technical merit, feasibility, and commercial potential;" Phase II awards of $750,000-$1,700,000[126] for two years to support successful efforts initiated in Phase I; and Phase III, which is not funded by SBIR dollars, to pursue commercialization.[127] The program issues a higher number of Phase I awards but allocates

[123] *First Quarter Recommendations*, NSCAI at 41-43 (Mar. 2020), https://www.nscai.gov/reports.

[124] OUSD(R&E) could leverage existing Intergovernment Personnel Act authorities as well as the pilot Public-Private Talent Exchange Program. See: *Department Of Defense Public-Private Talent Exchange (PPTE) Program: Questions/Answers*, Defense Civilian Personnel Advisory Service, (Aug. 23, 2018), https://www.dcpas.osd.mil/Content/Documents/PPTEQuestions_Answers23Aug2018.pdf.

[125] "As of November 2019, agencies may issue a Phase I award (including modifications) up to $256,580 and a Phase II award (including modifications) up to $1,710,531 without seeking SBA approval. Any award above those levels will require a waiver." About, Small Business Innovation Research (last accessed Sept. 3, 2020), https://www.sbir.gov/about.

[126] Id.

[127] Non-SBIR funding may be placed on an SBIR contract to further mature a technology, and this non-SBIR funding is not subject to any dollar limitations. NSCAI Staff Engagement, September 23. For more, see *About*, Small Business Innovation Research (last accessed Sept. 3, 2020), https://www.sbir.gov/about.

more funding towards Phase II, with the goal of placing many small bets on novel technologies and only scaling those that show real promise.[128]

The Small Business Administration serves as the coordinating agency and issues an annual policy directive derived from statute, but each Federal agency administers its individual SBIR program, designates R&D topics for solicitations, and vets company proposals. This structure provides Federal agencies the autonomy to tailor programs, thus, performance and results vary significantly.

The DoD's SBIR program is the nation's largest, awarding around $1.8 billion in SBIR contracts annually. However, the program suffers from common problems in transitioning successful prototypes, scaling solutions, and synchronizing investments. Contracts are complicated, and the current funding scale does not justify the hours of labor for new companies to fill out multi-volume reports and compliance documents. In some cases, overly prescriptive solicitations and lengthy award and decision periods discourage non-traditional vendors.[129] These challenges, paired with departmental incentive structures that can drive metrics of success based on the number of contracts rather than technology produced, have incurred the program reputational issues. Stakeholders across the Department acknowledge that too many Phase I SBIRs are awarded, often indiscriminately, yet note that if all Phase Is transitioned that would likely indicate that not enough risks were being taken.[130]

Furthermore, DoD's program is overwhelmingly geared towards laboratory research and technology proof of concept. SBIRs have become an effective means of outsourcing contract research, which can be an important part of the R&D process, but does not address the full scope of their congressional mandate.[131] If optimized, SBIRs can provide DoD a mechanism to collaborate with emerging technology startups across a range of technology readiness levels, and incentivize entrepreneurs to experiment with novel technology solutions to meet military problem sets and build future capabilities.

There has been recent momentum across the Services to use SBIR awards to develop and scale solutions from companies outside the defense industrial base. Dr. Will Roper, Assistant Secretary of the Air Force for Acquisition, Technology and Logistics, has led the charge for the Air Force, introducing high-value third phase contracts, SBIR Open Topics, and AFVentures.[132] The Army's new Special Program Awards for Required Technology Needs (SPARTN), jointly led by Assistant Secretary of the Army (Acquisition, Logistics &

[128] At a scale of about 1.8:1. In 2018, SBA reported 3123 Phase I awards across the program and 1711 Phase II awards. For the DoD, it was 1106 to 820. *Award Data*, Small Business Innovation Research (last accessed Sept. 17, 2020), https://www.sbir.gov/sbirsearch/award/all/?f%5B0%5D=itm_field_award_yr%3A2019.

[129] NSCAI staff engagements (Sept. 25, 2020; Sept. 28, 2020).

[130] This sentiment was shared across several engagements between July 1 and September 25, 2020.

[131] "The mission of the SBIR/STTR programs is to support scientific excellence and technological innovation through the investment of Federal research funds in critical American priorities to build a strong national economy. The program's goals are to: Stimulate technological innovation. Meet Federal research and development needs. Foster and encourage participation in innovation and entrepreneurship by women and socially or economically disadvantaged persons. Increase private-sector commercialization of innovations derived from Federal research and development funding." *About*, Small Business Innovation Research (last accessed Sept. 3, 2020), https://www.sbir.gov/about.

[132] NSCAI staff engagements (Aug. 27, 2020; Aug. 28, 2020). For more on Air Force efforts to stimulate small business partnership, see Theresa Hitchens, *Air Force to Pump New Tech Startups with $10M Awards*, Breaking Defense (Feb. 25, 2020), https://breakingdefense.com/2020/02/air-force-to-pump-new-tech-startups-with-10m-awards/. For more on SBIR Open Topic, see *SBIR Open Topic*, Air Force, AFWERX (last accessed Sept. 4, 2020), https://www.afwerx.af.mil/sbir.html.

Technology) and the AAL, "brings fast capital and access to end users and decision makers so innovators can build the right solution, and become a long-term Army client."[133] A smaller, focused program, SPARTN offers companies a clear and tiered pathway from prototype to acquisition.[134] The Navy has also focused heavily on scaling successful SBIR projects by bringing in program dollars earlier[135] and introducing new multi-million dollar rapid-funding opportunities.[136]

Phase II enhancements, sometimes called Phase IIB/II.5 contacts,[137] have become a common method to extend SBIR dollars to promising projects that fail to secure Phase III funding. The Navy Commercialization Readiness Program oversees the distribution of Phase II.5 contracts "to further develop SBIR technologies and to accelerate transition for existing Phase II projects."[138] The Air Force's AFWERX, Army, and DARPA, as well as several Federal agencies outside the DoD,[139] also use Phase IIB awards. However, current funding limits set by SBA reduce their efficacy by including Phase II enhancements under the Phase II cap of SBIR dollars.[140]

[133] U.S. Army, Army Applications Laboratory (last accessed Sept. 24, 2020), https://aal.army/.

[134] Phase I: "As many as 15 companies per SPARTN problem could receive a contract of up to $200,000 in non-dilutive capital for a 4-month period of performance." Phase II: "[F]ive companies per topic to receive up to $1.5 million" over 9-24 months. Post-phase II: Opportunity for "$2.5 million total value follow-on contract to build a prototype related to the specific problem." *SPARTN*, U.S. Army, Army Applications Laboratory (last accessed Sept. 24, 2020), https://aal.army/spartn/.

[135] NSCAI staff engagement (Sep. 3, 2020); Remarks by James Geurts, Assistant Secretary of the Navy for Research, Development, and Acquisition, delivered at the Pallas Foundation event on Innovation and Modernization in the Navy (Aug. 20, 2020).

[136] Via Broad Agency Announcements (BAAs), Department of Navy SBIR FY20.4 seeks proposals from innovative small businesses and startups for high-impact, scalable technologies that address both naval requirements and the needs of the commercial market. It offers funding up to $30 million. Graham Plaster, *Navy - New Small Business Funding Opportunity*, Defense and Intelligence Innovation Ecosystem (May 15, 2020), https://diie.substack.com/p/navy-new-small-business-funding-opportunity.

[137] These terms are used differently throughout DoD and can refer to a sequential/second Phase II, or cross-agency award. "Most agencies prefer to modify existing contracts to add funding, which reduces the workload on Contracting shops. Adding SBIR funds may require a waiver. Increasing an existing contract also is preferred to "save" the sequential Phase II to further mature the technology with SBIR funds. Enhancement programs require matching funds from a non-SBIR source." NSCAI staff engagement (Sept. 23, 2020).

[138] The Navy Commercialization Readiness Program was "created as part of section 252 of the National Defense Authorization Act of Fiscal Year 2006," and "set-aside is 1% of the available SBIR funding to be used for administrative support to accelerate transition of SBIR developed technologies." *Navy Phase II.5 Structure and CRP*, U.S. Navy, (last accessed Sept. 16, 2020), https://www.navysbir.com/cpp.htm.

[139] Other Federal agencies have more successfully leveraged SBIR as a tool to "stimulate technological innovation" and "meet Federal research and development needs." *About*, Small Business Innovation Research (last accessed Sept. 3, 2020), https://www.sbir.gov/about. The National Cancer Institute (NCI) awards $12 million across ten projects through its SBIR Phase IIB Bridge Award, predicated on the project's ability to "secure substantial independent third-party investors." "NCI intends to commit $12M for up to 10 new awards in FY2021." *Phase IIB Bride Award*, National Cancer Institute SBIR Development Center (July 22, 2020), https://sbir.cancer.gov/bridge. Similarly, the National Science Foundation provides partial matching through its Phase IIB supplement to "speed the commercialization" of technologies that excel in Phase I and II. "NSF may match 50 cents on every $1 of qualifying revenues or third-party investment (minimum match $50,000 and maximum $500,000) through a Phase IIB supplement." *America's Seed Fund SBIR/STTR, About*, National Science Foundation (last accessed Sept. 3, 2020), https://seedfund.nsf.gov/about/.

[140] According to the SBA's Office of Investment and Innovation policy directive: "while there is no limit on the number of such special/supplementary awards, there is a limit on the total amount of SBIR/STTR funds that can be administered through them—the amounts of these awards count towards the size of the initial Phase II or the sequential Phase II, each of which has a guideline amount of $1 million and a limit of $1.5 million." *Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Program Policy Directive*, SBA at 74 (May 2, 2019), https://www.sbir.gov/sites/default/files/SBIR-STTR_Policy_Directive_2019.pdf.

Small changes in how SBIR contracts are vetted, prioritized, and transitioned will provide outsized dividends. It would not necessitate a policy change, but rather reorient departmental procedures to align with the mission of the legislation to support U.S. private sector innovation.[141] First, SBIR awards should be issued more discriminately, and where appropriate, aligned with OUSD(R&E)'s modernization priorities and their accompanying R&D Objectives described above. Second, promising SBIR projects must be given sufficient financial and institutional support to simultaneously develop their technology and their business.

The National Defense Authorization Act for Fiscal Year 2017 moved oversight of the DoD's SBIR program offices from the Office of Small Business Programs to the Office of Research, Technology, and Laboratories (RT&L) within the OUSD(R&E) to facilitate SBIR's role as a tool to "stimulate technological innovation" and "meet Federal research and development needs."[142] RT&L's responsibilities include ensuring S&T priorities are focused on modernization, as outlined in the 2018 National Defense Strategy. As such, Small Business and Technology Partnerships (SBTP) is conducting an inventory of its programs, including SBIR, and categorizing by modernization topic.[143] It also introduced new vehicles for SBIR dollars to help bridge the gap between SBIR-funded Phase II contracts and non-SBIR funded Phase III. The Office of the Secretary of Defense (OSD) Transitions SBIR Technology (OTST) Pilot Program provides SBIR awardees the opportunity to apply for "an interim technology maturity phase (Phase II), inserted into the SBIR development."[144] SBTP is working with SBIR program officers to align these enhancement awards with modernization priority roadmaps, as detailed above in Recommendation 6.

The OTST pilot, along with the dedicated AI transition fund outlined in Tab 2, will provide financial incentives to leverage the SBIR program for AI. To further focus the program on developing new AI capabilities, rather than applying commercial technology to military use cases, OUSD(R&E) could also introduce a special solicitation on AI that invites solutions across a diversity of AI approaches[145] and a range of technology readiness levels.[146]

[141] See *About*, Small Business Innovation Research (last accessed Sept. 3, 2020), https://www.sbir.gov/about.

[142] *Defense Primer: Under Secretary of Defense for Research and Engineering*, Congressional Research Service (Feb. 4, 2020), https://fas.org/sgp/crs/natsec/IF10834.pdf; *About*, Small Business Innovation Research (last accessed Sept. 3, 2020), https://www.sbir.gov/about.

[143] See examples of tagging in TechLink study of FY 2011-2016 Rapid Innovation Fund (RIF) participants. *Defense Rapid Innovation Fund, An Assessment of RIF Effectiveness FY 2011-2016*, DoD RIF Program (July 2020), https://www.dodrif.us/Account/Login.

[144] The OTST Pilot Program includes two (2) Transition Funding Strategies: Phase II Enhancement (e) funding is applied to a Phase II or II contract. The OSTP program offers up to $1.0M in matching funds to the Assistant Director's (AD) or Funding Sponsor of the current SBIR contract. OSTP program offers Accelerated Transition (AT) funding, not to exceed $1.7M in matching SBIR dollars, for Funding Sponsor who are committed to transition the SBIR Technology and have already identified acquisition funding. The sponsor enters into a Technology Transition Agreement (TTA) with the OTST program, showing proof of the acquisition plan and sufficient additional funding to reach transition. Susan Celis, *Department of Defense Small Business Innovation Research (SBIR) Small Business Technology Transfer (STTR) Program Overview*, U.S. Department of Defense at 169 (July 22, 2020), https://www.sbirroadtour.com/wp-content/uploads/2020/08/2020-Virtual-SBIR-Weeks-5-Minute-Pitch-Slides.pdf.

[145] The future will likely be defined by a fusion of many different AI approaches including expert systems, model-based AI, symbolic-based AI, statistical machine learning, and new and evolving AI approaches such as neuro-symbolic AI. See neuro-symbolic research at *Neuro Symbolic AI*, MIT-IBM Watson AI Lab (last accessed Oct. 5, 2020), https://mitibmwatsonailab.mit.edu/category/neuro-symbolic-ai/.

[146] DARPA's SBIR program, for example, is unique in its long time horizon. Most of its investments are pre-commercial and will take another 8-10 years to develop before results can be scaled for military or commercial use.

Other adjustments must take place for the program to support entrepreneurship: contracts must be easier to understand and fill out, review periods shortened and clearly communicated, and oversight streamlined to keep pace with the current rate of technology innovation. Recent restrictions on the number of Phase II prototyping contracts a company can receive, aiming to cut down on "SBIR mills,"[147] need to be paired with sufficient commercialization or transition support for successful prototypes to scale into programs of record. This means 1) providing, or facilitating, sufficient funding to reach a viable product and company, and 2) assessing companies both on their product and business growth potential.

SBIR funds provide non-recurring engineering dollars to early-stage companies to get them off the ground, but they ultimately need recurring revenue to survive. If the goal of DoD's SBIR program is pre-commercial investments in technologies with potential national security applications, it should equip awardees with the tools to eventually *realize* commercialization or transition within the Department. This means connecting awardees with "customers" earlier in the process. In some cases, defense and non-defense "customers" can be introduced as early as Phase I. In other cases, large Phase II and IIB/II.5 contracts are necessary to reach a viable product, but SBIR programs can earn buy-in from potential customers through matching program funds.[148] The pathway to transition, including milestone criteria and dollar amounts, should be communicated clearly to SBIR awardees so that they can plan and resource accordingly.

Requirements of matching private-sector funding earlier in the SBIR process[149] can serve as a proxy to vet commercialization potential, as well as a means to facilitate external support for business development, but it should not come at the expense of independent due diligence. SBIR phases are structured to enable proof of concept before further government investment. Determinations of "commercial potential" should go beyond the technology and research, to assess the health of the business. Phase II and supplemental awards should be based on a broader diligence process that includes the long-term health and viability of the company. This assessment should consider as a starting point the firm's technical capabilities, financial structure, management structure, and the larger commercial market opportunities.

Proposed Executive Branch Action

The Commission recommends the DoD allocate a portion of SBIR funding for scaling successful SBIR projects through Phase II enhancements.[150] Funding waiver limits[151] should be scaled appropriately, following best practices set by Services and OSD.[152] Additionally,

[147] Some SBIR contracts have been abused as a vehicle for single-use companies. This has led to the derogatory term, "SBIR mills," referring to companies that win many SBIR awards but do not transition or advance the technology.
[148] Critically, with the growth of dual-use technologies, larger SBIR and matching funds should not be seen as competing with commercial investment, providing non-dilutive capital that crowds interested investors.
[149] The Air Force tried to require match funding as part of phase II for its STRATFI program but was limited by a phrase in the SBIR policy directive that distinguished Phase IIB awards by this requirement. See recommended executive branch action below.
[150] Including the OTST pilot and Phase B/II.5 awards in OSD and the Services.
[151] *Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Program Policy Directive*, SBA (May 2, 2019), https://www.sbir.gov/sites/default/files/SBIR-STTR_Policy_Directive_2019.pdf.
[152] The Air Force's Strategic Finance (STRATFI) program offers rewards of up to $15 million, with 1:1:2 Program-SBIR-Private Matching options. *Air Force Pivots to Virtually Connect Defense Innovators, Announces 'Big Bets,'* U.S. Air Force AFWERX (Mar. 13, 2020), https://www.af.mil/News/Article-Display/Article/2111607/air-force-pivots-to-virtually-connect-defense-innovators-announces-big-bets/.

SBA should amend its Policy Directive to allow programs to require matching private sector funds as early as Phase II.[153]

Furthermore, the Commission recommends OUSD(R&E) align the Department's SBIR awards with the modernization priorities and their accompanying technical road maps in order to focus investments on subsets of key technologies on which private sector R&D can help advance.

Recommendation 8: Launch an AI Catalyst Initiative

The global competition in AI is fierce and ongoing; where the government cannot compete in scale of investment, it can compete in speed and strategy.[154] In complement to the ongoing pathfinder efforts to source existing technology solutions from the private sector, there is a need to explore novel pathways for DoD to work with the private sector on early-stage AI R&D, to harness the cutting-edge expertise where it resides in the private sector to build towards future game-changing capabilities.

Overseen by a joint council composed of OUSD(R&E), the Joint AI Center (JAIC), and Service leadership, the AI Catalyst Initiative (AICI) would bring together government and industry in a unique configuration to research, develop, and demonstrate cutting-edge AI technology. In contrast to China's efforts to employ a growing number of companies to advance Party-state and military purposes, this Initiative would celebrate the autonomy of America's private sector as a vehicle for technological breakthrough via competitive, flexible R&D agreements.

As conceived, the Initiative would fill a gap in DoD's current approach. Whereas many DoD pathfinder organizations and contracted R&D projects emphasize the development of narrowly-defined, near-term solutions, AICI would accelerate research with industry into longer time horizon, next-generation capabilities—supporting the evolution from basic research to easily scalable prototypes.[155] Furthermore, while other DoD multi-participant partnership programs tend to concentrate on academia and lack tight coordination with end users, AICI would couple operators and private-sector researchers to smooth the transition of

[153] On page 74 of the SBA SBIR/STTR Policy Directive, the line "For example, some agencies administer Phase IIB awards that differ from the base Phase II in that they require third party matching of the SBIR/STTR funds" could be changed to "For example, some agencies administer Phase II or IIB awards that require third party matching of the SBIR/STTR funds." *Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Program Policy Directive*, SBA at 74 (May 2, 2019), https://www.sbir.gov/sites/default/files/SBIR-STTR_Policy_Directive_2019.pdf.

[154] As cited in the Commission's *2019 Interim Report*: "China has overseen a 30 times increase in its overall R&D funding from 1991 to 2015, and is projected to surpass the United States in absolute R&D spending within 10 years. . . . Chinese tech firms have reached enormous scale and are poised to become leaders in applied AI, excelling in numerous commercial AI applications, including in healthcare, education, and e-commerce. Some of these applications may pose national security risks. . . . China is intensifying efforts to exploit civilian and commercial developments in AI and leveraging a growing number of companies to advance Party-state and military purposes." See *Interim Report*, NSCAI at 17-18 (Nov. 2019), https://www.nscai.gov/reports.

[155] For example, the Air Force's AFWERX initiative or Navy's NavalX Tech Bridges create linkages between companies (often small business concerns) and internal United States Government partners; however, the goal is either to grow these businesses by supporting them as they win contracts, or to deliver products that fill an immediate need. AICI is complementary to this style of government-industry partnership—it takes the long view, accelerates research in addition to product delivery, and drives both collaboration and competition. For more on NavalX Tech Bridges, see *Spanning the Gap: Tech Bridges*, NavalX (last accessed Sept. 15, 2020), https://www.secnav.navy.mil/agility/Pages/techbridges.aspx.

promising concepts into fieldable solutions.[156] Likewise, AICI confers more structure, end-user interaction, and multi-year experimentation than do canonical "grand challenge" programs.

At a strategic level, AICI would be executed by DARPA or the Services' innovation entities.[157] Partnerships with two or more private sector companies[158] would be formed around key research priorities, informed by OUSD(R&E) modernization roadmaps, Service needs, and a gap analysis of current DoD efforts to advance priority subsets of AI technology.[159] Over multiple years, teams would initiate research into these critical areas, ultimately developing a series of outputs available for follow-on production contracts from Service components.[160]

The Initiative would derive impact from its tight coupling between end-users and developers and flexible approach to private sector innovation. The Commission's *Second Quarter Recommendations* note that AI development should be accompanied by "early delivery of minimally viable products to the end user to ensure AI-enabled solutions solve the right problems and are easily accessible." Iterative R&D with regular feedback from operational users would be baked-in to the AI Catalyst Initiative. Moreover, the broad scope of each project's problem-set would encourage bold thinking from industry while ensuring that deliverables add value to U.S. national security— "structured serendipity," as one stakeholder the Commission spoke to put it.[161]

[156] For example, the Defense Enterprise Science Initiative (DESI), a successful basic research pilot that partners industry firms and academic research institutions, focuses on use-inspired basic research but does not create pathways for consistent association with operators. See *Defense Enterprise Science Initiative (DESI)*, DoD OUSD(R&E) (last accessed Sept., 30, 2020), https://basicresearch.defense.gov/Programs/Defense-Enterprise-Science-Initiative/.

[157] Such as AFWERX, SOFWERX, NavalX or the Army Applications Lab.

[158] These teams could be formed naturally (i.e., industry gets in touch with industry) or artificially (DoD matches companies to each other and to projects). The former concept is best exemplified by the DoD's Mentor-Protege program, which encourages small businesses to seek out partnership with large traditional contractors, or the STTR program. The latter concept could follow the model set forth by the MIT-Air Force AI Innovation Accelerator. The accelerator receives proposals from both the Air Force and MIT, matches projects, and then vets and narrows based on merit and subject. On the whole, a team-based model could incite friction between participants and serve as a disincentive for prospective companies, but would bolster cross-fertilization of ideas and potentially decrease cost for DoD. These consortia may also be better suited to a longer-term (6 year) project timeline and to multidisciplinary projects. For more on STTR, see Recommendation 7.

[159] In matching companies with DoD counterparts, AICI could again parallel the MIT-Air Force Accelerator's model of connecting Air Force sponsors to relevant academic projects. AF teams have the option of sponsoring projects that they deem significant to their mission—in the long-run, this sponsorship signals AF interest in the project and expedites transition of viable solutions. See Rob Matheson, *MIT and US Air Force sign agreement to launch AI accelerator*, MIT News (May 20, 2019), https://news.mit.edu/2019/mit-and-us-air-force-sign-agreement-new-ai-accelerator-0520. The selected research topics would be generated using input from end users as well as the USG R&D community, Services, Combatant Commands, and OSD. The themes would be informed by OUSD(R&E) modernization roadmaps and gap analysis of current DoD efforts to advance priority subsets of AI technology.

[160] As currently envisioned, the project would not constrain teams to develop a single product ready for testing and fielding, as is often the case under the current contracted R&D regime. Instead, companies would be expected to apply innovative insights to produce multiple prototypes and proofs-of-concept (which may differ in level of sophistication or technology readiness) for DoD consideration—as a company would do in the commercial sector with a new line of products.

[161] NSCAI stakeholder engagement (Sept. 2, 2020).

Key elements of the Initiative include:

1. **Non-traditional Contractors.** The Initiative would strive to access a diverse base of private sector companies. Participants would span large, medium, and small firms, as well as both traditional and nontraditional defense companies.

2. **Strategic Investments.** Placing multiple, big bets in a diversified portfolio of key players in the AI community maximizes the probability that a company produces successful project outputs. The companies would be competitively accepted to AICI and matched with components based on research prowess, promise, and subject matter specialty.

3. **Diversity of AI Methods**. AICI will promote research across a variety of AI methods, noting that future breakthroughs will likely rely on a fusion of today's prominent statistical machine learning with various model-based, symbolic-based, or alternate future approaches.

4. **Existing Authorities.** By creatively leveraging existing agreement constructs, the Initiative would work within the system to enable the rapid implementation of research projects. No new contracting vehicles would be required, reducing time and bureaucratic hurdles to implementation.[162]

5. **Collaboration.** Given the scope of the Initiative, DoD could support participants by facilitating access to data, matching teams with secure development environments, and offering co-location privileges at government research departments.

The program would run for between five and seven years. While the total cost is heavily dependent on the configuration details selected for the Initiative (e.g., number of participants), anticipated expenditures would amount to between $100 and 250 million.

Proposed Executive Branch Action

The Commission recommends that the Secretary of Defense establish a multi-year AI Catalyst Initiative led by OUSD(R&E) and set aside appropriate funding, estimated between $100 and 250 million, pursuing research priorities based on the gap analysis conducted by OUSD(R&E). The Initiative should leverage existing authorities in novel configurations to

[162] A prime example is potential use of Consortium Other Transactions (OTs). Consortium OTs present capabilities well-suited to the iterative, interactive development of AI and emerging technologies. In addition to supporting federal partnership with more than one private sector firm (i.e., teams), Consortium OTs also confer a tabula rasa for agreement negotiation and, notably, introduce an OT "basket" provision. This provision allows for the "storage" of prototypes and products not funded immediately upon completion of the project. For example, if a funded team develops four promising prototypes, but only two are transitioned immediately into programs of record, the other two would remain in the bucket for three years in the case of available funding or greater interest in the product. See *Other Transaction Agreements*, Medical CBRN Defense Consortium (last accessed Sept. 30, 2020), https://www.medcbrn.org/ota/.

stimulate and adopt the results of industry innovation, introducing creative solutions for next-generation national security needs.

TAB 2 — Applying Artificial Intelligence for National Security Missions

The aggressive investments and approach our competitors have made in artificial intelligence (AI) and advanced technologies and the explosion of private sector research and development in today's globalized technology marketplace have fundamentally changed the character of global competition and conflict.[163] To maintain advantage in a technological competition with near-peer competitors, the Department of Defense (DoD) and the Intelligence Community (IC) must organize for speed and agility, integrating the perspectives of technologists and operators at every level. The DoD and the IC must have empowered Chief Technology Officers who understand global trends in technology innovation and can effectively align strategy, investments, and policy to ensure the delivery of game changing technologies to the warfighter at the speed of relevance.

Although the Commission's mandate is focused on AI and associated technologies, the Commission recognizes that many of the challenges associated with accelerating technology in DoD and the IC are not unique to AI. In the first quarter, the Commission assessed that the DoD efforts to adopt and integrate AI applications face substantial structural obstacles.[164] These obstacles significantly inhibit its progress by preventing AI strategy from being effectively implemented and by impeding tech breakthroughs in the lab and private sector from translating into results in the field. Therefore, in order to speed adoption of AI, it is necessary to address shortcomings in the broader technology ecosystem.

In this report, the Commission proposes options to maximize the impact of DoD's Chief Technology Officer (CTO), the Under Secretary of Defense for Research & Engineering (USD(R&E)), and to designate an IC CTO. Collectively, these options will drive closer coordination with the military services and intelligence entities as they conduct reach and development (R&D), planning, budgeting, and acquisition activities; and provide funding mechanisms to incubate and mature promising technology that would otherwise not make it from lab to field. These recommendations build on the Commission's *First Quarter (Q1) and Second Quarter (Q2) Recommendations*, which focused on senior leadership through a Tri-Chair Steering Committee, a Technology Annex to the National Defense Strategy (NDS), and elevating the Joint Artificial Intelligence Center (JAIC) to report directly to the Secretary of Defense.[165]

The seven options below are not mutually exclusive from one another or from the recommendations made in the First and Second Quarters. Rather, our Q3 draft recommendations are crafted to build upon our previous work.

[163] *Summary of the 2018 National Defense Strategy of the United States of America*, U.S. Department of Defense at 2-3 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[164] The Commission's *First Quarter Recommendations* noted that these obstacles include: inadequate policy and governance structures, unclear and/or mis-aligned authorities; insufficient infrastructure, and an antiquated and overly cumbersome acquisition system. See *First Quarter Recommendations*, NSCAI at 15 (Mar. 2020), https://www.nscai.gov/reports.

[165] See *First Quarter Recommendations*, NSCAI at 15-19 (Mar. 2020), https://www.nscai.gov/reports; *Second Quarter Recommendations*, NSCAI at 22-33 (July 2020), https://www.nscai.gov/reports.

Part I — DoD: Introduction and Background

China and Russia are developing and fielding advanced kinetic and non-kinetic capabilities to attack us simultaneously in all domains, drive wedges between our forces, and undermine our conventional deterrence. In addition to deploying advanced military capabilities in eastern Ukraine and Syria, Russia has used emerging technologies, information operations, and "gray zone" tactics below the threshold of war to discredit and subvert democratic processes in Georgia, Ukraine, and elsewhere.[166] Concurrently, China is pursuing a comprehensive military modernization effort to deny the U.S. access to the region while employing political and economic coercion of neighboring countries to increase its influence in the Indo-Pacific region and weaken our own.[167]

Today's military-technical environment presents a fundamentally different challenge for the DoD than the Cold War era, when most of the advances in military capabilities were purpose-built and the product of military laboratories. As the National Defense Strategy (NDS) states, competitive advantage is no longer assured by whoever develops disruptive technologies first, but rather by those militaries that are better able to integrate those technologies and adapt their way of fighting.[168]

The United States has experienced a similar imperative before. In the inter-war period of the 1920s and 1930s, for example, significant advances were made in a range of new technologies and weapons, including aircraft, mechanization, radio, and radar. Every military had access to these very same tools, but not every power was able to harness those new technologies and develop effective new ways of fighting such as the Germans did with Blitzkrieg, the American Navy did with carrier warfare, or the British did with an integrated air defense system.[169] In the late 1970s, Defense Secretary Harold Brown, and his Under Secretary of Defense for Research and Engineering, William Perry, looked at the Soviet three-to-one advantage in conventional forces arrayed along the inner-German border and realized they needed to take decisive action. They looked to emerging technologies to provide the means to restore the conventional military balance.[170] They developed a strategic technology plan to support their "offset" strategy that identified and pursued stealth, new precision guided munitions, and advanced intelligence, surveillance, and reconnaissance capabilities.[171] Those powerful new capabilities provided the Joint Force dominant military advantage for nearly four decades.

[166] See *Summary of the 2018 National Defense Strategy of the United States of America*, U.S. Department of Defense at 2 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf [*hereinafter* 2018 National Defense Strategy]; Kathleen H. Hicks, *Russia in the Gray Zone*, Center for Strategic and International Studies (July 25, 2019), https://www.csis.org/analysis/russia-gray-zone.

[167] 2018 National Defense Strategy at 2.

[168] Id. at 10.

[169] Williamson R. Murray & Allan R. Millett, *Military Innovation in the Interwar Period*, Cambridge University Press at 6-49, 191-226, 265-299 (1996). See also Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military*, Cornell University Press (1991).

[170] See Edward Keefer, *Harold Brown: Offsetting the Soviet Military Challenge, 1977-1981*, Secretaries of Defense Historical Studies at 575-576 (2017); see also Robert Tomes, *The Cold War Offset Strategy: Origins and Relevance*, War on the Rocks (Nov. 6, 2014), https://warontherocks.com/2014/11/the-cold-war-offset-strategy-origins-and-relevance/.

[171] See id. As noted in the Commission's *Interim Report*, the past two decisive military technological revolutions, known as the "first offset" and the "second offset, were enabled by specific technological breakthroughs that solved core defense problems. The reference here is to the "second offset," in which the U.S. drove and exploited innovations in emerging and enabling technologies to restore a credible deterrent against a nuclear Soviet Union. See *Interim Report*, NSCAI at 29 (Nov. 2019), https://www.nscai.gov/reports [hereinafter *Interim Report*].

It is important to note that Brown and Perry confronted the Soviet Union at the height of the Cold War when the two rivals were locked in a dynamic military-technical competition with enormous implications. Secretary Brown was determined that the Department's R&D efforts transitioned fast into actual operational systems and so provided Perry with considerable acquisition authority.[172] Perry occupied the number three position in the Department and was equal in status to the Service secretaries.[173] He met daily with the Secretary of Defense and roughly monthly with the President.[174] From that empowered position in the Office of the Secretary of Defense (OSD), Secretary Perry was able to aggressively drive the Department's R&D strategy and acquisition choices by the military Services. Brown and Perry identified the most demanding operational challenges NATO would face in a conventional war versus the Warsaw Pact, developed a vision of potential technological solutions, and then focused the Pentagon's vast research and development community to devising solutions.

In its *Second Quarter Recommendations*, the Commission recommended the DoD produce a classified Technology Annex as a means to identify, develop, field, and sustain critical emerging and enabling technologies.[175] As Brown and Perry did in the 1970s with the Soviet threat, the Commission aimed to focus the defense enterprise on pursuing technology to solve the most complex challenges facing the Joint Force, connecting the priority operational challenges identified in the 2018 NDS to capability and concept development. While the Annex will help the Department prioritize key technologies, there must be a clear steward of these technologies to coordinate across the enterprise and ensure their delivery. As the DoD's Chief Technology Officer, the USD(R&E) has the mandate and authority to perform this function,[176] however more must be done to improve USD(R&E)'s efficacy.

How Did We Get Here? Congress' Vision for Military-Technical Superiority and the Creation of USD(R&E)

The National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2017 directed the dissolution of DoD's centralized acquisition office, which was responsible not only for defense acquisitions, program management, and logistics, but also the DoD's technology enterprise, including research and development.[177] Driven by concern over the eroding U.S. military advantage and the need to leverage new technologies, lawmakers argued that the Department's acquisition office had become too big and that its centralized authority created

[172] Edward Keefer, *Harold Brown: Offsetting the Soviet Military Challenge, 1977-1981*, Secretaries of Defense Historical Studies at 101 (2017).
[173] The Roles and Authorities of the Director of Defense Research and Engineering, Defense Science Board at 29 (Oct. 2005), https://dsb.cto.mil/reports/2000s/ADA440086.pdf. This stands in stark contrast to today when the third ranking civilian position in the Department is the Chief Management Officer, a position focused on business reform and cost cutting—it is not a position intended to drive innovation.
[174] *The Roles and Authorities of the Director of Defense Research and Engineering*, Defense Science Board at 30 (Oct. 2005), https://dsb.cto.mil/reports/2000s/ADA440086.pdf.
[175] *Second Quarter Recommendations*, NSCAI at 24-26 (July 2020), https://www.nscai.gov/reports.
[176] Department of Defense Directive (DoDD) 5137.02 authorizes the USD(R&E), as a Principal Staff Assistant (PSA) reporting directly to the Secretary of Defense, to promulgate DoD policy within the responsibilities, functions, and authorities assigned therein. For the full list of responsibilities and functions, see *Under Secretary of Defense for Research And Engineering (USD(R&E))*, DoDD 5137.02 (July 15, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/513702p.pdf?ver=2020-07-15-124712-047.
[177] Pub. Law 114-238, National Defense Authorization Act for Fiscal Year 2017 (2016), https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf.

bureaucratic obstacles to delivering critical capabilities.[178] To better organize DoD for the changing threat environment, Congress reestablished USD(R&E) with a mission to advance technology and innovation.[179] Simultaneously Congress also established a separate Under Secretary of Defense for Acquisition and Sustainment (A&S), aiming to "foster distinct technology and acquisition cultures to better deliver superior capabilities."[180]

In conference reports from the FY 2017 NDAA proceedings, legislators in both the House and the Senate articulated a clear vision for R&E. The Senate Armed Services Committee, for example, noted the historical importance of the role of USD(R&E), and set an expectation that "just as previous USD (R&E) incumbents led the so-called 'Second Offset' strategy, which successfully enabled the United States to leap ahead of the Soviet Union in terms of military technology, the new USD (R&E) would be tasked with driving the key technologies that must encompass what defense leaders are now calling a 'Third Offset' strategy."[181] Similarly, the House Armed Services Committee expected that the new R&E would "take risks" and "push the technology envelope."[182]

Lawmakers established R&E with a broad purview. The 2017 NDAA gives USD R&E the following duties and powers: "(1) serving as the chief technology officer of the DoD with the mission of advancing technology and innovation for the military services and DoD; (2) establishing policies on, and supervising all defense research and engineering, technology development, technology transition, prototyping activities, experimentation, and developmental testing activities and programs, including the allocation of resources for defense research and engineering, and unifying defense research and engineering efforts across DoD; and (3) serving as the principal advisor to the Secretary on all research, engineering, and technology development activities and programs in DoD."[183]

Based on this Congressional mandate, the Department tasked R&E with responsibilities and

[178] See e.g., Kathleen J. McInnis, *Goldwater-Nichols at 30: Defense Reform and Issues for Congress*, Congressional Research Service at 1 (June 2, 2016), https://fas.org/sgp/crs/natsec/R44474.pdf (noting that DoD officials themselves saw opportunities to reduce bureaucratic burdens associated with the acquisition office). These proposed changes included, but are not limited to: reducing the number of stakeholders on the Defense Acquisition Board which, at the time of the report publishing, had reached approximately 35; and streamlining documentation, including by pushing authorities and responsibilities for relevant acquisition decisions to the military services and creating enterprise-wide resources for acquisition data reporting. Id. at 31.

[179] The House Armed Services Committee's conference report for the FY 2017 NDAA notes that three broad priorities framed conference discussions around reorganizing USD(AT&L): "(1) elevate the mission of advancing technology and innovation within the Department; (2) foster distinct technology and acquisition cultures to better deliver superior capabilities for the armed forces; and (3) provide greater oversight and management of the Department's Fourth Estate." See H. Rept 114-840 for the National Defense Authorization Act for Fiscal Year 2017, (Nov. 30, 2016), https://www.congress.gov/congressional-report/114th-congress/house-report/840.

[180] The Department rechartered the new acquisition office as an enabling organization, responsible for providing best practices, policy, and products designed to improve speed and affordability of capability delivery. A&S maintained oversight of joint programs, but decision authority for most other major defense acquisition programs was delegated to the military services—a move that significantly strengthened the role of the armed services in the acquisition process relative to the Office of the Secretary of Defense. See *Report to Congress, Restructuring the Department of Defense Acquisition, Technology and Logistics Organization and Chief Management Officer Organization*, U.S. Department of Defense (Aug. 2017), https://dod.defense.gov/Portals/1/Documents/pubs/Section-901-FY-2017-NDAA-Report.pdf [hereinafter 2017 AT&L Reorganization Plan]; see also Peter Modigliani, *After the Divorce: How the Pentagon Can Position Itself for Speed, Agility, and Innovation in the New Era of Acquisitions*, The MITRE Center for Technology & National Security (Mar. 2019), https://apps.dtic.mil/sti/pdfs/AD1107958.pdf.

[181] See *Defense Primer: Under Secretary of Defense for Research and Engineering*, Congressional Research Service (Feb. 4, 2020), https://fas.org/sgp/crs/natsec/IF10834.pdf (quoting S. Rpt. 114-255).

[182] Id.

[183] Id.

functions that the Commission has identified as critical to advancing AI and other emerging technologies. These include addressing novel, technology-related threats; setting technical direction and driving the DoD investment strategy; and marrying new technology concepts with warfighter feedback.[184]

In its *First Quarter Recommendations*, the Commission stated that to accelerate the application of AI and emerging technology for competitive advantage, DoD must have an integrated approach that coordinates emerging technology across the lifecycle of research, development, and fielding.[185] R&E has taken important steps towards achieving this vision. As noted in Tab 1, USD(R&E) has identified 11 technology focus areas for the Department based on the NDS, including AI/ML.[186] The principal director for each technology area is responsible for "unifying and advancing the Department's investments and capabilities in that area," and "ensur[ing] the transition of technologies into operational use."[187]

Below, the Commission proposes options to maximize the impact of R&E's work to date, driving closer coordination with the military services as they conduct R&D, planning, budgeting, and acquisition activities; and providing mechanisms to incubate and mature promising technology that would otherwise not make it from lab to field.

Recommendation 1: USD(R&E) should integrate DoD's technology scouting community of practice, leveraging AI-enabled analytics to provide authoritative technology inputs for national security planning.

The technological competition for leadership in AI and related technologies requires developing and executing an effective national strategy. The U.S. strategic approach relies on the independence and entrepreneurial spirit of American industry and the free economic systems of our allies and partners around the world. To effectively leverage the innovations from this global economic system requires a sophisticated technical intelligence program that monitors developments across the progression from basic research to prototyping to fielding capabilities. This intelligence must be global in scale, monitoring emerging technologies in near real time, especially in the rapidly evolving field of AI. The intelligence must be actionable, allowing decision makers to continuously update technology roadmaps for our national security agencies without lengthy time lags.

Developing a technology strategy that maintains competitive advantage in today's globalized technology marketplace requires three fundamental elements of technical intelligence: (1) an understanding of the future threat capabilities that China and Russia have in their R&D pipelines; (2) an understanding of future friendly capabilities in U.S. and allied R&D pipelines; and (3) an understanding of emerging military and dual use technologies worldwide available for inclusion into national security capabilities. The scientists and engineers spread across the DoD and service labs comprise the most knowledgeable community anywhere for assessing the prospects of emerging technologies for DoD use.

[184] For the full list of responsibilities and functions, see *Under Secretary of Defense for Research And Engineering (USD(R&E))*, DoDD 5137.02 (July 15, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/513702p.pdf?ver=2020-07-15-124712-047.

[185] *First Quarter Recommendations*, NSCAI at 15 (Mar. 2020), https://www.nscai.gov/reports.

[186] See *Modernization Priorities*, U.S. Department of Defense, USD R&E, (last accessed Sept. 30, 2020), https://www.cto.mil/modernization-priorities/.

[187] Id.

However, their technical skills must be merged with the operational experience of warfighters, the collection skills of intelligence professionals, and the analytic skills of data scientists.

In its response to the 2017 NDAA provision creating USD(R&E), the DoD specified that the new organization would organize around three major themes. The first was a Strategic Intelligence Analysis Cell (SIAC) that would "focus on understanding the enemy's capabilities and vulnerabilities, conducting analysis on our own U.S. capabilities, tracking technology trends across the globe and assessing potential/emerging threats and/or future opportunities that warrant action, that merit investment."[188] However, since the establishment of USD(R&E), the SIAC has been downgraded from a direct report to the Under Secretary and largely focused on examining threat technologies for OSD customers.[189]

In its *Second Quarter Recommendations*, the NSCAI recommended that the DoD, with support from the Office of the Director of National Intelligence (ODNI), produce a classified Technology Annex that charts a clear course for identifying, developing, fielding, and sustaining critical emerging and enabling technologies.[190] Developing and maintaining this annex will require significant coordination among USD(R&E), USD(A&S), CAPE, and the armed services.

For the USD(R&E) to fulfil its role in implementing the NDS; i.e., the generation and execution of technology roadmaps, it should establish SIAC as a robust analytic hub that marshals DoD, IC, and interagency technology scouting capabilities for strategic effect.[191] To achieve this, the Commission proposes assigning USD(R&E) as the Executive Agent responsible for producing the Technology Annex, providing a tool for USD(R&E) to set the agenda in developing the DoD's technology priorities and investment strategy. The Commission further recommends reestablishing the SIAC Director as a direct report to the USD(R&E) in alignment with the strategic intent of the 2017 NDAA.

SIAC should serve as the hub for an interagency and international technology scouting community of practice. There are organizations at nearly every level of DoD that conduct technology scouting activities according to their mandate or in support of their mission areas. OSD and service laboratories, warfighting concept developers, and IC agencies have long monitored technology developments with small dedicated staff, including overseas personnel

[188] See *Report to Congress, Restructuring the Department of Defense Acquisition, Technology and Logistics Organization and Chief Management Officer Organization*, U.S. Department of Defense at 8 (Aug. 2017), https://dod.defense.gov/Portals/1/Documents/pubs/Section-901-FY-2017-NDAA-Report.pdf [hereinafter 2017 AT&L Reorganization Plan]

[189] Both the Department's congressionally-required 2017 AT&L Reorganization Plan and subsequent reporting, including a primer published by the Congressional Research Service, indicated that SIAC would be a direct report to the USD(R&E). However, SIAC currently reports through the Deputy Director for Engineering and the Director of Defense Research and Engineering for Advanced Capabilities. See *Defense Primer: Under Secretary of Defense for Research and Engineering*, Congressional Research Service (Feb. 4, 2020), https://fas.org/sgp/crs/natsec/IF10834.pdf.

[190] *Second Quarter Recommendations*, NSCAI at 24-25 (July 2020), https://www.nscai.gov/reports.

[191] USD(R&E) has the mandate and authority to perform this function. See *Under Secretary of Defense for Research And Engineering (USD(R&E))*, DoDD 5137.02 at 5-6 (July 15, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/513702p.pdf?ver=2020-07-15-124712-047.

to monitor international activity.[192] Integrating these efforts would be a force-multiplier, informing and speeding development of the Technology Annex, while creating a sustainable community of practice to support strategic technology scouting efforts in DoD and the IC over the long-term. Findings from an effective technology scouting program will drive R&D investments into the emerging technologies with the highest potential.

SIAC should be provided with increased funding to allow expanded investments in AI tools, commercial data, and a military technology fellows program. SIAC should develop enterprise resources for use by the DoD's entire technology community, including AI-enabled analysis of large commercial databases, classified threat intelligence, and the technology investment portfolios of the United States Government and its allies. SIAC should also employ these resources internally, producing dashboards and other strategic intelligence for senior DoD leadership.

SIAC should convene an interagency technology scouting community of practice from the service laboratories, OSD (including the Defense Applied Research Projects Agency and the Defense Innovation Unit), the Departments of Energy and Homeland Security, university affiliated research centers, and federally-funded research and development centers, combatant commands, and international security partners. This community of practice should join USD(R&E) in developing federated approaches for producing the Technology Annex, conducting future technology wargames and analytic exchanges, engaging with industry and updating requirements for technology scouting tools and data. As active participants in producing the Technology Annex, members of the community of practice should be empowered to act on analytic conclusions from the Annex as they are developed, updating their R&D priorities in real time and thereby speeding the United States Government's response to emerging technology threats and opportunities. Additional mechanisms for translating findings from technology scouting into rapid action are contained in Tab 1 of this memo.

USD(R&E) should merge the perspectives of technologists and warfighters from the outset in this technology scouting function. A short-term technology fellowship program achieves this with minimum disruption to military manning cycles, while maximizing the number of operators exposed to the gamut of emerging technology opportunities examined in technology scouting. Circulating warfighters through USD(R&E)'s technology scouting program will create a feedback loop between operational commands and DoD laboratories at the action officer level, helping to ensure that USD(R&E) strategic investments and recommendations are grounded in operational realities, and reducing the potential for technological surprise by raising awareness of the technology landscape within the operational community.

SIAC should establish a technology fellows program, inviting organizations in the tech scouting community to nominate personnel for short term (three to twelve month) assignments with SIAC where they would work side-by-side with SIAC analysts. The fellows program should be designed to achieve two goals:

[192] These bespoke efforts focused on technology requirements for individual agencies suffer from a common set of limitations: 1) they are a step removed from the core mission (R&D for laboratories, operations, and threats for the IC) and therefore their budgets always get squeezed first, and 2) they are small, isolated organizations without the critical mass of resources needed to make significant investments in data, tools, and methods.

1. Improve the speed and quality of the United States Government's response to AI and related emerging technologies with national security application. Technology scouting collaboration at the action officer level would speed the United States Government response to emerging technology opportunities and threats by ensuring that situational awareness from these activities is shared immediately across the community, vice waiting for approval and publication of the formal Technology Annex. Technology fellows would provide SIAC with the capacity to build interdisciplinary teams to conduct in depth investigations of emerging technologies, initiating direct contacts with researchers and vendors in addition to passive data collection. Expanding and diversifying the technology scouting workforce will ensure critical evaluation of emerging technologies and their potential applications from a range of operational, institutional, scientific, and engineering perspectives.

2. Develop personnel with greater understanding of emerging technologies across the national security community. Technology fellows would be immersed in the process of observing and analyzing the technology landscape, increasing their technical literacy and currency. They would develop professional contacts across a broad range of organizations and technology disciplines. Military personnel selected for the fellows program would develop a joint perspective on technology solutions, and inject warfighting perspectives into the DoD's technology scouting activities. Upon completion of the program, these personnel would be prime candidates for concept development, prototyping, and experimentation activities in the services and the joint force. The technology fellows program should leverage hiring authorities from the Public-Private Talent Exchange (PPTE) Program and the Intergovernmental Personnel Act (IPA) to allow inclusion of tech fellows from the Defense Industrial Base, technology industries, academia, and other government agencies as required to ensure access to non-DoD research and perspectives.[193]

Proposed Executive Branch Action

The Commission recommends that the Secretary of Defense direct the following actions:

- Assign USD(R&E) as the Executive Agent responsible for producing the Technology Annex.

- Reestablish the SIAC Director as a direct report to the USD(R&E).

- Increase funding for SIAC's technical intelligence project over the Future Years Defense Program (FYDP) to allow expanded investments in AI tools, commercial data, and a technology fellows program.

- SIAC should develop enterprise resources for use by the DoD's entire technology community, including AI-enabled analysis of large commercial databases, classified

[193] Tab 3 of this report addresses related issues, such as: career fields that would allow individuals to focus on digital skills throughout a career; the need for Additional skill identifiers (ASI), Additional Qualification Designations (AQD), Additional Military Occupational Specialty (AMOS), and Special Experience Identifiers (SEI) to track and manage personnel with skills and experience; and the creation of billets that require personnel to have achieved an emerging technologies qualification prior to assignment.

threat intelligence, and the technology investment portfolios of the United States Government and its allies.

- SIAC should convene an interagency technology scouting community of practice from the service laboratories, OSD (including the Defense Applied Research Projects Agency and the Defense Innovation Unit), the Departments of Energy and Homeland Security, university affiliated research centers, and federally-funded research and development centers, combatant commands, and international security partners.

- SIAC should establish a technology fellows program, inviting organizations in the technology scouting community to nominate personnel for short term (three to twelve month) assignments with SIAC where they would work side-by-side with SIAC analysts. The fellows program should be designed to achieve two goals: 1) to improve the speed and quality of the United States Government's response to AI and related emerging technologies with national security application, and 2) develop personnel with greater understanding of emerging technologies across the national security community.

Recommended Legislative Action

The Commission recommends that Congress appropriate an additional $10 million to USD(R&E)'s budget to support expanded SIAC technology scouting capabilities and a technology fellows program.

Recommendation 2: USD(R&E) should be appointed the Co-Chair and Chief Science Advisor to the Joint Requirements Oversight Council (JROC) for Joint and cross-domain capabilities.

To accelerate application of AI and other emerging technologies for competitive advantage, USD(R&E) must play a central role in connecting technological advancements in research and development to joint operational requirements. Within USD(R&E) the Principal Director for AI has the responsibility to set the technical direction and ensure the transition of AI-enabled technologies into operational use.[194] Empowering USD(R&E) to inform operational requirements in the Joint Requirements Oversight Council (JROC) remains complementary to the Commission's recommendation to elevate the JAIC as a direct report to the Secretary of Defense and enables JAIC to focus on rapid delivery of AI-enabled applications to the warfighter now.

[194] See *Modernization Priorities*, U.S. Department of Defense, USD(R&E) (last accessed Sept. 30, 2020), https://www.cto.mil/modernization-priorities/.

As the decision authority for the bulk of the Department's major defense acquisition programs (MDAPs), the Services currently have primary responsibility for the system architectures of their respective domain capabilities sometimes to the detriment of joint warfighting interoperability. Although the Services have recognized the primacy of digital interoperability particularly in the area of Joint All Domain Command and Control, many legacy Service systems and networks continue to hinder the movement of data at machine speed. Data from myriad sensors and platforms across all our warfighting domains remains locked in proprietary systems and thus made unusable by AI technologies. Development of a truly integrated, joint network that enables AI and machine teaming requires common data standards, open architecture systems, and API-driven interoperability.

The Department understands the urgent imperative to realize this type of cross-service and all-domain systems integration for use on the future battlefield. The Secretary of Defense directed the Joint Staff to develop a new Joint Warfighting Concept (JWC) by December of this year. A key characteristic of the concept is eliminating service stovepipes, allowing the joint force to operate seamlessly, across all domains and in highly contested environments.[195] To maintain overmatch in the rapidly changing threat environment, DoD must remain laser-focused on this vision and take bold steps to enforce it through the DoD requirements process. USD(R&E) should be appointed as co-chair and Chief Science Advisor to the JROC for this express purpose.

As the JWC is finalized, the JROC will outline what is required to enable the concept, defining joint capabilities and functions and developing requirements guidance that the services will use as they develop and deploy systems to meet joint needs.[196] In order to perform its core duty of ensuring U.S. military technical superiority, USD(R&E) must play a key role in this process. As Chief Technology Officer, USD(R&E) should draft the technical guidance for the JWC, partnering closely with the JROC community to understand warfighter needs and leveraging awareness of global technology trends, threats, and adversary capabilities to validate technical feasibility of requirements developed by the services.

The JROC is chaired by the Vice Chairman of the Joint Chiefs of Staff (VCJCS) and is responsible for validating requirements to close an identified gap in joint military capabilities.[197] The VCJCS is pursuing a variety of JROC reforms to right size the

[195] The Vice Chairman of the Joint Chiefs of Staff makes this point frequently. See e.g., Theresa Hitchens, *New Joint Warfighting Plan Will Help Define "Top Priority" JADC2: Hyten*, Breaking Defense (Jan. 29, 2020), https://breakingdefense.com/2020/01/new-joint-warfighting-plan-will-help-define-top-priority-jadc2-hyten/. Most recently, in a speech at the DoD's JAIC Symposium on July 10, VCJCS Hyten noted that "the amazing thing about the Joint Warfighting Concept is that it eliminates all the lines on the battlefield . . . ." See Remarks by General John E. Hyten to the Joint Artificial Intelligence Symposium and Exposition (Aug. 9, 2020), https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2344135/remarks-by-general-john-e-hyten-to-the-joint-artificial-intelligence-symposium/.

[196] The JROC's mission includes but is not limited to: "(1) [a]ssessing joint military capabilities, and identifying, approving, and prioritizing gaps in such capabilities, to meet applicable requirements in the National Defense Strategy" and "(2) [r]eviewing and validating whether a capability proposed by an Armed Force, Defense Agency, or other entity of the DoD fulfills a gap in joint military capabilities." See *Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)*, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5123.01H at A-1(Aug. 31, 2018), https://www.acq.osd.mil/jrac/docs/CJCS-Instruction-5123.01H.pdf [hereinafter CJCSI 5123.01H].

[197] Importantly the CJCSI defines the term "joint military capabilities" as "collective capabilities across the joint force, including both joint and force-specific capabilities that are available to conduct military operations." CJCSI 5123.01H at A-4.

organization and develop requirements to enable the JWC. He has stated his objective is "empower[ing] the JROC process to do what the JROC was intended to do," referring to the Council's duty to verify that capabilities proposed by the services meet joint requirements as well as integrating such capabilities for joint functions.[198] As the co-chair and Chief Science Advisor, USD(R&E) could provide increased assistance to the VCJCS in this effort and, in particular, on the integration of service-developed capabilities for joint functions. Joint functions, including C2, logistics, and data access, refer to cross-service, cross-domain capabilities that will enable the U.S. military to operate as a cohesive, joint force. The joint functions will be central to the JWC; however, these types of mission-oriented, cross-domain capabilities are underserved in the JROC process—challenged by the priorities and funding of the military services.[199] USD(R&E) should serve as the JROC champion and systems architect for those mission-oriented, cross-domain challenges demanding a joint technical solution that no one service can solve alone.[200]

As stated in the Commission's *Second Quarter Recommendations*, effective integration of emerging technology requires close collaboration between technologists and warfighters.[201] Strengthening R&E's role in the JROC would connect operators to the whole of the Department's S&T enterprise, including innovation hubs such as the Defense Innovation Unit and Defense Innovation Board, to help solve joint technical warfighting challenges and close capability gaps. It would also bolster shared accountability for NDS outcomes by assigning clear responsibility to USD(R&E) to help the joint staff interpret and translate the JWC into technical guidance and encouraging USD(R&E) to participate fully in the activities of the JROC's supporting organizations such as the Joint Capabilities Board and Functional Capabilities Boards (FCBs).[202]

Proposed Executive Branch Action

To ensure USD(R&E) can fulfill its role as CTO and best support the JROC, the Commission recommends that the Secretary of Defense task USD(R&E) with responsibility to develop the technical guidance for the JWC and supporting concepts. The technical

[198] Theresa Hitchens, *New Joint Warfighting Plan Will Help Define "Top Priority" JADC2: Hyten*, Breaking Defense (Jan. 29, 2020), https://breakingdefense.com/2020/01/new-joint-warfighting-plan-will-help-define-top-priority-jadc2-hyten/.

[199] The VCJCS has referred to joint functions including C2, logistics, and joint information access, as "lost children" in the JROC process, meaning that no one service is responsible for delivering that function for the joint force. See Theresa Hitchens, *New Joint Warfighting Plan Will Help Define "Top Priority" JADC2: Hyten*, Breaking Defense (Jan. 29, 2020), https://breakingdefense.com/2020/01/new-joint-warfighting-plan-will-help-define-top-priority-jadc2-hyten/.

[200] For joint C2 in particular, the Department has made an effort to put a clear governance structure in place by establishing a cross-functional team (CFT) to guide the technical implementation for the Joint All Domain Command Control (JADC2) concept. The CFT is co-lead by the joint staff and DoD CIO office with USD(R&E) as an advisor. This structure, while a step in the right direction, does not elevate USD(R&E) to a leadership position commensurate with its role as Chief Technology Officer. It is expected that JADC2 will be designated a joint supporting concept under the JWC. As such, the JROC will become responsible for validating that the system design and approach are set up to meet the joint need for all-domain, integrated command and control. USD(R&E) should co-lead this effort with the joint staff, focusing on providing technical expertise to ensure synchronization with other emerging technologies such as AI.

[201] See *Second Quarter Recommendations*, NSCAI at 22-33, (July 2020), https://www.nscai.gov/reports.

[202] Secretary of Defense Mark Esper has championed the need for shared responsibility to move the Department forward. See *Secretary of Defense Mark T. Esper Message to the Force on Accomplishments in Implementation of the National Defense Strategy*, U.S. Department of Defense (Jul. 7, 2020), https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2266872/secretary-of-defense-mark-t-esper-message-to-the-force-on-accomplishments-in-im/.

guidance developed by USD(R&E) should be broad, embrace best practices from industry, enable iterative development approaches, and provide an ability to evolve and adapt as technology progresses. USD(R&E) should develop such guidance in close coordination with the Joint Staff and the Combatant Commands as the end-users of joint capabilities and with input from key stakeholders such as the DoD CIO and CDO, service CIOs and CDOs; as well as implementing partners in the JAIC and military services. The guidance should marry technical direction and system requirements with expertise derived from technology scouting efforts and the contents of the Technology Annex to the NDS. In addition, the Secretary should ensure:

- DoD updates the JROC charter to reflect USD(R&E) as the co-chair and Chief Science Advisor with responsibility for: (1) validating the technical feasibility of requirements developed by the services and ensuring they meet the broad technical guidance; and (2) delivering technology assessments and trend reports that inform JROC deliberations on future military requirements.[203]

- USD(R&E) participates at every level of the JROC, providing expertise to support program planning and system architecture and identifying opportunities to reduce redundancies across the services for joint function, including through "systems of systems" that can meet joint capability needs and are not joint programs of record.

Proposed Legislative Branch Action

Congress should update title 10. Section 181 to designate USD(R&E) Co-Chair and Chief Science Advisor to the Joint Requirements Oversight Council.

Recommendation 3: USD(R&E) should have a dedicated fund to mature, operationally prototype, and transition exceptionally promising AI-enabled technologies.

DoD's budget process poses a significant obstacle to transitioning advances in the lab to capabilities in the field.[204] The current defense budget process requires that funds be requested two years in advance of their execution and focuses planning within the five-year FYDP. This means that program managers must predict technology innovation years ahead of time—a practice that is challenging for traditional defense S&T and particularly problematic for fast-moving technologies such as AI.[205] It also means that DoD's planning process focuses on a five-year horizon, even when technology development may not align predictably with that timeframe. Under this system, and given today's rate of technological change, program managers will increasingly struggle to rapidly identify, fund, and incorporate promising technologies into their programs. Without pre-planned program funds

[203] The JROC charter designates USD(R&E) as an advisor to the Council on "matters within [its] authority and expertise." See CJCSI 5123.01H at A-3. However, it does not clarify what is meant by "advisor" and to what extent R&E input should be considered relative to service or joint staff technology leads. In contrast, the charter clearly denotes that input from another advisor group, the service Chiefs of Staff, shall be sought after and strongly considered due to their role as the end consumer of the acquisition. See id.

[204] The Commission's *Second Quarter Recommendations* noted this challenge, focusing on the tension the sequential nature of DoD's budget construct places on iterative technologies such as AI. See *Second Quarter Recommendations*, NSCAI at 16 (July 2020), https://www.nscai.gov/reports.

[205] Eric Lofgren, *The "Valley of Death" and the PPBS in Defense Technology Transition*, Acquisition Talk (Nov. 4, 2018), https://acquisitiontalk.com/2018/11/the-valley-of-death-and-the-ppbs-in-defense-technology-transition/.

available at the end of a defense S&T project's life cycle, the technology can stall or be abandoned before it's potential can be evaluated in a realistic environment.[206]

The rapid pace of development of AI and other emerging technologies highlights weaknesses of defense planning on a five-year cycle, which can lead to prioritizing predictable, incremental technological progress over transformative capabilities. To move as fast as our competitors and maintain the defense advantage, DoD must have a means to support promising AI projects beyond early-stage research and development even when planned program funding is not yet in place.

To ensure the transition of critical AI-enabled technologies, USD(R&E) should have a dedicated fund to continue AI projects with outsized potential that may not have an identified source of program funding as they near the end of their S&T lifecycle. The fund should be used to conduct operational prototyping and speed the transition of AI-enabled applications into both service-specific and joint mission capabilities.[207] The fund would effectively "bridge the gap," allowing program managers time to request and program money for integration of the technology into their programs of record. Additionally, access to the fund would buy down risk for the military services and allow OSD to support transformational and joint AI capabilities for the Services to adopt through transition.[208]

Part of Congress' original vision for USD(R&E) was that it would place strategic bets on key capability-enabling technologies that the military services or private sector may not fund.[209] The dedicated fund would better equip R&E to perform this function. In conjunction with recommendations 1 and 2 above, which respectively call for a strengthened role for USD(R&E) in technology scouting activities as well as the DoD requirements process for joint or cross-domain capabilities; the fund will equip USD(R&E) with needed leverage to truly advance AI application, spanning the gap until program funds are available for the technology. Importantly, the House Armed Services Committee (HASC) acknowledged the need for such a mechanism.[210] In their recent report, the HASC Future of Defense Task Force recommended restoration of the Department's Rapid Innovation Fund to "assess,

[206] As technology matures it progresses through different subsets of Research, Development, Test, and Evaluation (RDT&E) appropriations. "S&T" refers to a specific subset of DOD RDT&E appropriations—budget activities 6.1, 6.2, and 6.3—that fund DOD basic research, applied research, and advanced technology development. At the end of "S&T," (funding for which is provided by an organization within the DoD or service R&D community) the next type of funding must be available to continue progressing the technology. These types of funds, used for advanced component development and prototyping, including operational prototyping, are traditionally held by DoD program offices. See John F. Sargent Jr., *Defense Science and Technology Funding*, Congressional Research Service (Feb. 21, 2018), https://fas.org/sgp/crs/natsec/R45110.pdf.

[207] Establishment of this fund would need to be accompanied with transfer authority such that USD(R&E) could provide the money to the services to conduct these activities.

[208] The Strategic Capabilities Office pioneered this approach by focusing on ways to "to reduce upfront risk on potentially game-changing concepts that can be fielded in the near-term." See *Fiscal Year (FY) 2019 President's Budget Operation and Maintenance, Defense-Wide*, U.S. Department of Defense at OSD-670 (Feb. 2018), https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/OSD_OP-5.pdf.

[209] This vision was emphasized in several NSCAI staff conversations with former Congressional staff and senior DoD officials. These thoughts are also reflected in the FY 2017 NDAA conference report, which stated that the conferees expected R&E to "take risks, press the technology envelope, test and experiment, and have the latitude to fail, as appropriate." See *Defense Primer: Under Secretary of Defense for Research and Engineering*, Congressional Research Service (Feb. 4, 2020), https://fas.org/sgp/crs/natsec/IF10834.pdf.

[210] *Future of Defense Task Force Report 2020*, U.S. House Committee on Armed Services (Sept. 23, 2020), https://armedservices.house.gov/_cache/files/2/6/26129500-d208-47ba-a9f7-25a8f82828b0/6D5C75605DE8DDF0013712923B4388D7.future-of-defense-task-force-report.pdf.

fund, and accelerate innovative technology solutions for the warfighter," and noted the fund is a "critical pathway for relevant late-stage technologies to be funded inside the Department of Defense."[211]

Proposed Executive Branch Action

In the near-term, the Commission recommends that the Secretary of Defense establish the fund as a pilot under the management of USD(R&E) to mature, operationally prototype, and transition exceptionally promising AI-enabled technologies. DoD should work with the Office of Management and Budget to pursue Congressional support for the pilot and include approximately $200 million for the fund in the FY 2022 budget request. Establishing the fund as a pilot at this amount would allow the Department to test its utility on a smaller scale and prove to appropriators that USD(R&E) can appropriately manage more flexible funding mechanisms.[212] In use of the fund, the Commission recommends:

- USD(R&E) should work closely with the JAIC, the Joint Staff, and the military services to identify specific programs and mission areas ripe for potential application of AI technologies, with particular attention to near-term, emerging warfighter needs, and use the fund to accelerate efforts in those areas.[213]

- The Department should establish clear metrics for success and frequently engage the Congressional defense committees to maintain transparency and report progress.[214] If successful, over the long-term the USD(R&E) should work with the Deputy Secretary and Secretary of Defense to establish several similar funds within USD(R&E) for different portfolios of critical emerging technologies.

[211] Id. at 9. Between FY 2011 and FY 2019, Congress provided the Department money under a "Rapid Innovation Fund" to accelerate the transition of innovative technologies into defense acquisition programs to meet urgent needs. Congress did not provide funding for the program in the FY 2020 NDAA, but directed a study to assess the effectiveness of the fund. The study found that between FY 2011 and FY 2016, over 50% of RIF awards have or are expected to transition to military use. Amounts appropriated to the fund between FY 2012 and FY 2019 ranged between $175 million to $200 million. *Defense Rapid Innovation Fund: An Assessment of RIF Effectiveness FY 2011-2016*, U.S. Department of Defense at 7 (2020), https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2020/08/techlink_rif_report.pdf.

[212] There is recent precedent for the use of pilots to assess the effectiveness of alternative funding mechanisms. For example, the Department's Budget Activity 8 (BA 8) pilot proposal, which the Commission endorsed in its *Second Quarter Recommendations*, was supported in H.R. 7617, a minibus of spending bills for FY 2021. H.R. 7617 included funding for eight of the Department's nine proposed pilots under the BA 8 construct. BA 8, which would give the DoD the ability to fund the full acquisition lifecycle of software for select pilot programs out of a single spending category, is intended as a first step towards a new spending category that will streamline the acquisition process for software. See Billy Mitchell, *DoD Has OMB Support for Special Software-Only Appropriations Pilots*, FedScoop (Sept. 10, 2019), https://www.fedscoop.com/dod-omb-support-special-software-appropriations-pilots/; *Second Quarter Recommendations*, NSCAI at 18 (Jul. 2020), https://www.nscai.gov/reports.

[213] Implementation of recommendations 1 and 2 in this Tab would aid USD(R&E) in performing this function by driving closer synchronization with the military services.

[214] Frequent, transparent communication with Congress arose in multiple interviews conducted by NSCAI staff as a primary ingredient for success when pursuing more flexible funding mechanisms. This sentiment was echoed on a recent podcast episode where Air Force Ventures co-founders stated, "It really comes down to the relationship between the legislative and executive branch. One of the things we've been trying really hard to do is get as much information and as much transparency out about what we're doing as possible. We spend a lot of time preparing briefings. [...] As long as you do that, you allow people to build trust in what you're doing. Congress can fulfill their oversight responsibility." See Eric Lofgren, *How AFWERX transitions tech with Chris Benson, Steve Lauwer, and Jason Rathje*, Acquisition Talks (July 6, 2020), https://acquisitiontalk.com/2020/07/how-afwerx-transitions-tech-with-chris-benson-steve-lauver-and-jason-rathje/.

Proposed Legislative Branch Action

Congress should direct the Secretary of Defense to establish a dedicated fund administered by OUSD(R&E) to mature, operationally prototype, and transition exceptionally promising AI-enabled technologies.

Part II — Intelligence Community: Introduction and Background

Intelligence leaders see great potential in AI for IC applications. The CIA's Deputy Associate Director for Learning, Joseph Gartin, has written that "intelligence analysis is at an inflection point" with a future that will be shaped by AI, big data, and machine learning.[215] AI-enabled tools can be applied to multiple stages of intelligence collection, processing, and operations to gain efficiencies as well as uncover patterns and trends not obvious to human analysts. AI-enabled tools can provide cognitive automation of human sensory processing through natural language processing and audiovisual analysis, vastly reducing the burden of manual processing and freeing analysts for higher level work. For example, advances in speech to text transcription and language analytics now enable reading comprehension, question answering, and automated summarization of large quantities of text.[216] There is also promising research into AI-enabled approaches to authorship attribution based on linguistic analysis which has great potential for the IC.[217]

AI-enabled tools can also assist with video data processing, identifying the key frames worthy of further human analysis and relieving the burden of human analysts watching hundreds of hours of irrelevant video.[218] For example, in a 2017 Posture Statement for the Senate Armed Services Committee, the commander of U.S. Central Command testified that his organization has daily requirements for over 2,800 hours of full-motion video.[219] If we assume a human analyst could watch 10 hours of video per day, that means it would take 280 intelligence professionals just to watch the raw footage each day, before even beginning any true analysis or applying human judgment.

Similarly, AI-enabled tools also have great potential to augment filtering, flagging, and triage across multiple types of bulk signals intelligence data-sets. Such tools can identify connections and correlations within and between bulk data-sets more efficiently and at a greater scale than human analysts are capable of doing, and can flag those findings and the most important content for further human analysis. Such tools can also use algorithms for behavioral analytics to generate predictions about future human behavior.[220] For example,

[215] Joseph Gartin, *The Future of Analysis*, Studies in Intelligence at 1 (June 2019), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-63-no-2/pdfs/Future-of-Analysis.pdf.

[216] Alexander Babuta, et al., *Artificial Intelligence and UK National Security*, Royal United Services Institute for Defence and Security Studies at 11 (Apr. 2020), https://rusi.org/publication/occasional-papers/artificial-intelligence-and-uk-national-security-policy-considerations.

[217] Id.

[218] Id. at 12.

[219] *Statement of General Joseph L. Votel on The Posture of U.S. Central Command*, U.S. Central Command (Mar. 19, 2017), https://www.centcom.mil/ABOUT-US/SASC-POSTURE-STATEMENT-2017/.

[220] Alexander Babuta, et al., *Artificial Intelligence and UK National Security*, Royal United Services Institute for Defence and Security Studies at 12-14 (Apr. 2020), https://rusi.org/publication/occasional-papers/artificial-intelligence-and-uk-national-security-policy-considerations.

AI-enabled tools can be effective in signal detection and early warning by recognizing deviations from baseline normal behavior and activities.[221]

AI-enabled analysis of open source intelligence (OSINT) also has vast potential for the IC. It is important to note that OSINT is not limited to traditional media sources (newspapers, radio broadcasts, etc.) and social media. OSINT also includes publicly available information such as public government data sources (official reports, budget documents, hearing testimonies, etc.), professional and academic publications, commercial data sources (industry reports, financial statements, commercial imagery, etc.), and more. AI-enabled tools can ingest high volumes of data from all of these sources and find trends and patterns that produce valuable intelligence insights that may not be discovered by human analysts. AI-enabled analysis of open source and publicly available information can also generate predictive analysis, giving the potential to "warn regional commanders of upcoming political protests, political violence, extremist attacks or other kinds of security related events [that] could take place."[222] In a 2019 Foreign Affairs article, former Central Intelligence Agency (CIA) Deputy Director Michael Morrell and Hoover Institute Senior Fellow Amy Zegart characterized the challenges and opportunities of leveraging open source intelligence, noting that "the U.S. intelligence community must figure out how to harness the open-source revolution and an array of other technologies faster and better than American adversaries. At the same time, it must balance this effort with its constitutional and ethical obligations to safeguard privacy and civil liberties."[223]

The 2019 National Intelligence Strategy of the United States of America acknowledges the importance of AI, automation, and augmentation to increase insight, knowledge, and speed in providing timely, relevant, and accurate analysis to decision makers.[224] It also stresses the importance of greater integration and coordination within the IC and outlines seven enterprise objectives, including an objective of integrated mission management and an objective of information sharing and safeguarding.[225]

The Augmenting Intelligence using Machines (AIM) initiative within the Office of the Director of National Intelligence (ODNI) provides the framework for that integration and coordination. The 2019 AIM Strategy assesses that AI, process automation, and IC officer augmentation (AAA) technologies are transformative elements critical for future mission success and efficiency, given the dramatic increases in the volume and velocity of data.[226]

[221] Brian Katz, *The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection*, CSIS Briefs (July 13, 2020), https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection.

[222] Nathan Strout, *AI Could Transform Open Source Intelligence in the Developing World*, C4ISRNET (Apr. 21, 2020), https://www.c4isrnet.com/artificial-intelligence/2020/04/21/ai-could-transform-open-source-intelligence-in-the-developing-world/.

[223] Amy Zegart & Michael Morrell, *Spies, Lies, and Algorithms*, Foreign Affairs (May/June 2019), https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms. In handling open source information on U.S. persons, IC agencies operate under guidelines approved by the Attorney General. See, e.g., David Kris, *The CIA's New Guidelines Governing Publicly Available Information*, Lawfare (Mar. 21, 2017), https://www.lawfareblog.com/cias-new-guidelines-governing-publicly-available-information.

[224] *National Intelligence Strategy of the United States of America*, Office of the Director of National Intelligence at 21 (2019), https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.

[225] Id. at 17.

[226] *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines*, Office of the Director of National Intelligence at iv (2019), www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf.

Recommendation 4: Within ODNI, the Director of S&T should be designated as the IC's CTO and empowered to enable the IC to adopt AI-enabled applications to solve operational intelligence requirements.

Ongoing reforms within ODNI are taking positive steps to elevate the importance of AI-enabled applications and associated technologies. These reforms seek to codify and elevate the AIM initiative.[227] The Commission encourage Congress and ODNI to go a step further in strengthening the role of the Director of S&T.

The Director of S&T is a statutory position in U.S. Code Title 50,[228] but the law does not specify that the position is the CTO for the IC, as the comparable Title 10 language does for USD(R&E) within DoD. Nor does Title 50 address precedence within ODNI. Most significantly, USD(R&E) has statutory authority to: "establish[] policies on, and supervis[e], all defense research and engineering, technology development, technology transition, appropriate prototyping activities, experimentation, and developmental testing activities and programs and unify[] defense research and engineering efforts across the Department."[229] No equivalent authority exists for the Director of S&T within ODNI.

Proposed Executive Branch Action

ODNI should consider the following recommendations to strengthen the Director of S&T:

- The Director of S&T should be designated as the IC CTO and granted additional authorities for establishing policies on, and supervising, IC research and engineering, technology development, technology transition, appropriate prototyping activities, experimentation, and developmental testing activities.

- The Director of S&T should be elevated to a Senior Executive Service (SES) position that reports directly to the DNI.

- The Director of S&T should have a fund that would allow the ODNI to identify and invest in AI applications with outsized potential that may not have an identified source of agency or program funding as they near the end of their S&T life cycle.

Proposed Legislative Branch Action

Congress should designate the Director of S&T within ODNI as the IC CTO and grant that position additional authorities for establishing policies on, and supervising, IC research and engineering, technology development, technology transition, appropriate prototyping activities, experimentation, and developmental testing activities.

[227] NSCAI staff engagements with multiple intelligence officials (Aug. 5, 2020; Aug. 7, 2020; Aug. 10, 2020; Aug. 12, 2020).

[228] 50 U.S.C. § 3030.

[229] 10 U.S.C. § 133a.

Recommendation 5: The IC CTO, in coordination with USD(R&E), should develop a technology annex to the National Intelligence Strategy that establishes technology roadmaps to adopt AI-enabled applications to solve operational intelligence requirements.

The IC has taken important steps in establishing the AIM initiative and publishing the 2019 National Intelligence Strategy for the United States of America. Now, it must focus on implementing those strategies in a coordinated way. Similar to the Commission's recommendation for the DoD, a technology annex to the National Intelligence Strategy can focus the IC on the development and fielding of critical technologies, such as AI. This annex and the DoD technology annex should be mutually supported and maintained through coordinated reviews and updates. The annex should identify emerging technologies and applications that are critical to enabling specific capabilities to address the IC's most pressing intelligence requirements. The main objective of the annex should be to chart a clear course for identifying, developing, fielding, and sustaining those critical emerging and enabling technologies, and to speed their transition into operational capability. The technology annex should set clear guidance that drives prioritization and resourcing, while allowing enough flexibility for disparate and decentralized entities to implement that guidance as best suits their organization.

Proposed Executive Branch Action

The IC CTO, in coordination with USD(R&E), should develop a technology annex to the National Intelligence Strategy that establishes technology roadmaps to adopt AI-enabled applications to solve operational intelligence requirements. The technology annex should generally mirror the Commission's recommended DoD technology annex and should, at a minimum, include:

- Identified intelligence support requirements, including how the IC analyzes the global environment and monitors technological advancements, adversarial capability development, and emerging threats.

- Identified functional requirements and technical capabilities necessary to enable concepts that address each challenge.

- A prioritized, time-phased plan for developing or acquiring such technical capabilities, that takes into account research and development timelines, a strategy for public private partnerships, and a strategy for connecting researchers to end users for early prototyping, experimentation, and iteration.

- Identified additional or revised acquisition policies and workforce training requirements to enable IC personnel to identify, procure, integrate, and operate the technologies necessary to address the intelligence requirements.

- Identified infrastructure requirements for developing and deploying technical capabilities, including data, compute, storage, and network needs; a resourced and prioritized plan for establishing such infrastructure; and an analysis of the testing, evaluation, verification, and validation (TEVV) requirements to support prototyping and experimentation and a resourced plan to implement them, including standards, testbeds, and red-teams for testing AI systems against digital “denial & deception” attacks.

- Consideration of human factor elements associated with priority technical capabilities, including user interface, human-machine teaming, and workflow integration.

- Consideration of interoperability with allies and partners, including areas for sharing of data, tools, and intelligence products.

- Flexibility to adapt and iterate annex implementation at the speed of technological advancement.

Proposed Legislative Branch Action

Congress should direct that the IC CTO develop a technology annex to the National Intelligence Strategy that establishes technology roadmaps to adopt AI-enabled applications to solve operational intelligence requirements.

Recommendation 6: The IC CTO should establish common technical standards and policies necessary to rapidly scale AI-enabled applications across the IC and have the authority to enforce them across the IC.

The ongoing reforms within ODNI also offer an opportunity for the IC, through AIM, to establish community-wide technical standards and policies that would enhance the IC’s ability to adopt AI-enabled technologies. For the IC to integrate AI-enabled applications into its operations, it must first establish and enforce common technical standards and policies. ODNI should establish these standards and policies in close coordination with industry, adopting those standards and practices that have emerged as best practices and industry standards. To ensure compliance, the Director of National Intelligence should have sufficient budgetary leverage, including the ability to fence or otherwise withhold funding. If the IC CTO determines that IC elements are not compliant with standards and policies, the IC CTO should be delegated authority to place a temporary hold on those IC elements ability to execute AI R&D funds until they demonstrate adherence. These standards and policies should be coordinated with USD(R&E) to maximize DoD and IC interoperability.

Proposed Executive Branch Action

At a minimum, the IC CTO should establish common technical standards and policies in the following areas:

- API driven architecture and associated policies that support the infrastructure to enable AI.

- Multi-level security standards for technical solutions to moving data across security clearance levels and the policies to enable it.

- Data tagging and labeling policies.

- Common standards for machine readable processing, exploitation, and dissemination (PED) products.

- Data sharing and access policies.

- Policies for an automated and reciprocal Authority to Operate (ATO) process that include rapid code certification & accreditation processes.

- Documentation strategies for data, models, and systems, and of the AI lifecycle, infrastructure to support traceability, training and testing procedures, human-AI design guidelines.[230]

- Technical standards for algorithms in support of interpretability and explanation, and policies to strengthen accountability.

- Technologies and operational policies that align with privacy preservation, fairness, inclusion, and human rights, documentation of value considerations and trade-offs.[231]

- Policies on alternative hiring authorities for term-limited appointments appropriate for technical positions, such as Special Government Employees (SGE), Highly Qualified Experts (HQE), and Intergovernmental Personnel Act (IPA) detailees.

- Policies to expand the use of prize challenges as alternatives to traditional procurement.

Proposed Legislative Branch Action

Congress should direct that the IC CTO develop the common technical standards and policies as outlined above.

Recommendation 7: The IC should develop a coordinated and federated approach to applying AI-enabled applications to open source intelligence.

While there will always be a need for traditional intelligence methods and classified intelligence, the IC must rethink integrating AI-enabled analysis of open source and publicly available information into all of its work streams. AI-enabled analysis of open source and publicly available information can expose patterns and trends that human analysts would not recognize, and should be used to inform all kinds of intelligence products.

In 2005, the IC established an Open Source Center (OSC) as a successor to the Foreign Broadcast Information Service (FBIS). Its mission was to collect and analyze open source information globally and across all media. In 2015, the OCS was renamed the Open Source

[230] NSCAI's *Second Quarter Recommendations* included thirty-two recommended practices for responsible AI across five disciplinary areas. See *Key Considerations for Responsible Development & Fielding of Artificial Intelligence*, NSCAI at 7-14 (July 22, 2020), https://www.nscai.gov/reports [hereinafter, *Key Considerations*].
[231] As outlined in *Key Considerations*.

Enterprise (OSE) and incorporated in the CIA's Directorate of Digital Innovation.[232] While the intent was for the OSE to remain the IC center of excellence and serve the entire community, some have argued that is not an effective construct. For example, Zegart and Morrell contend that:

> *On the organizational front, open-source intelligence deserves its own agency. Currently, its collection runs through the CIA's Open Source Enterprise, but this setup is akin to keeping the air force within the army, hobbling a new mission by putting it inside a bureaucracy that naturally favors other priorities. Secrets still reign supreme in the CIA, relegating open-source information to second-class status. Open-source intelligence will never get the focus and funding it requires as long as it sits inside the CIA or any other existing agency.*[233]

Proposed Executive Branch Action

The IC should develop a coordinated and federated approach to applying AI-enabled applications to open source intelligence. To achieve better coordination, ODNI should:

- Develop common standards and policies that enable the individual agencies to be more effective, such as contracting publicly available data sources for common use across the IC and clarifying or updating policy guidance on the appropriate use of publicly available and open source information, including with respect to privacy and civil liberties for U.S. persons or entities.

- Expand S&T intelligence on dual-use "emerging & disruptive technologies," with new billets for both collection and analysis.

- Support the IC by identifying reliable industry partners across the spectrum of information sources and creating contract vehicles to rapidly integrate them into intelligence work across the IC.[234] This should include establishing a pilot project to test "data-for-tools" exchanges in public-private partnerships.

- Aid the IC in communicating emerging risks and threats to industry and academia by coordinating the right expertise from across the IC—for example, by connecting non-government entities to the FBI for counter-intelligence guidance, or to U.S. Cyber Command/NSA for cybersecurity.[235]

[232] Steven Aftergood, *Open Source Center (OSC) Becomes Open Source Enterprise (OSE)*, Federation of American Scientists (Oct. 28, 2015), https://fas.org/blogs/secrecy/2015/10/osc-ose/.

[233] Amy Zegart & Michael Morrell, *Spies, Lies, and Algorithms*, Foreign Affairs (May/June 2019), https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms.

[234] As noted in a recent CSIS report: "High-end intelligence collection is no longer the sole domain of the U.S. IC and foreign intelligence rivals, as emerging technologies transform intelligence capabilities in the private sector. The commercialization of space and proliferation of satellite-based imaging and sensors will enable the commercial sector to collect quality GEOINT and SIGINT that, when combined with advanced analytics and OSINT data, can generate quality and timely all-source intelligence products. The IC could leverage the commercial sector not only for acquiring technology but also for collaboration or even outsourcing of collection, processing, and baseline analytic tasks while focusing the more 'exquisite' IC platforms on harder and priority targets." Brian Katz, *The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection*, CSIS Briefs (July 13, 2020), https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection.

[235] Because of digital connectedness, threats are now crossing institutional boundaries which the United States Government observes but many other nations do not. China will steal secrets from industry, creating a threat surface governed and protected more by the private sector than by the United States Government. That means the IC must provide intelligence to those private sector decision makers so they can make informed decisions. See

- Develop a robust capability for bringing in individuals without security clearances or awaiting security clearance adjudication and allowing them to work on unclassified projects that directly support the IC. The Commission's *First Quarter Recommendations* addressed the need for the creation of unclassified workspaces in DoD, the Department of Homeland Security, and the IC.[236] The Commission's recommendation is being addressed, in part, by the U.S. House of Representatives' FY 2021 NDAA bill, which directs DoD to develop guidance on the creation of unclassified spaces for personnel with pending security clearances.[237] However, the IC would also benefit from more opportunities for non-cleared people to work on national security issues. While there are pockets of successful initiatives, there is currently no systematic national level strategy for establishing an uncleared workforce.[238]

In addition, each individual agency should develop open source capabilities focused on the specialized applications of open source and publicly available information within their unique intelligence domains.

Proposed Legislative Branch Action

Congress should direct the IC to develop a coordinated and federated approach to applying AI-enabled applications to open source intelligence and integrating that into existing intelligence processes and products as outlined above.

Sue Gordon, *PDDNI Sue Gordon on the Intelligence Community's Imminent Information Challenges*, Intelligence Matters Podcast with Michael Morrell, CBS News (July 16, 2019), https://podcasts.apple.com/mt/podcast/pddni-sue-gordon-on-intelligence-communitys-imminent/id1286906615?i=1000444643764.

[236] See *First Quarter Recommendations*, NSCAI at 28 (Mar. 2020), https://www.nscai.gov/reports.

[237] See H.R. 6395, Sec. 243, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 116th Congress (2020).

[238] NSCAI staff engagements with multiple intelligence officials (Aug. 5, 2020; Aug. 7, 2020; Aug. 10, 2020; Aug. 12, 2020).

TAB 3 — Train and Recruit AI Talent

Part I: Recommendations to Strengthen the AI Workforce

For departments and agencies to become artificial intelligence (AI) effective enterprises, they must first overcome the challenge of developing an AI proficient workforce. United States defense and intelligence agencies need a workforce with expanded AI skills and expertise. Many end users will require minimal training and education, a topic the National Security Commission on Artificial Intelligence (NSCAI or the Commission) addressed in its *First Quarter (Q1) Recommendations*.[239] Others, however, will require more specialized training and education to buy, build, and use AI tools and AI related technology effectively and responsibly. Just as importantly, workforce development is a journey that will change as technology, missions, and organizational structures evolve. Today's workforce initiatives are helpful, but insufficient to meet the government's needs. Bolder, more aggressive actions are needed.

Creating a government workforce that is prepared to buy, build, and use today's digital technology is an immense challenge. The United States' education system does not produce enough digital expertise, and the government does not effectively recruit, train, or retain digital talent, or adequately capitalize on the available talent in the private sector or academia. These deficiencies have real and ongoing impacts on our national security. A more digitally proficient federal workforce will spend taxpayer dollars more efficiently, better secure our population and critical infrastructure, accelerate bureaucratic processes, and better represent American interests during negotiations with our partners, allies, and competitors.

NSCAI realizes the scale of the workforce problems facing the United States Government. Many of these issues are persistent and a holistic approach to changing the government workforce is necessary. These recommendations represent specific areas that, if enacted, would greatly improve the United States Government's workforce now and in the future. NSCAI will continue to evaluate challenges that face the national AI workforce and make recommendations to Congress that address challenges that prevent all Americans from participating in the AI workforce.

Components of an AI Workforce

As noted in the Commission's 2019 *Interim Report*:

> *National security organizations must have AI workforces capable of performing six functions: 1) planning and executing an organization-wide strategy; 2) purchasing and maintaining software and hardware infrastructure; 3) managing and analyzing data; 4) when necessary, developing software for unique needs; 5) performing verification, validation, testing, and evaluation; and 6) deciding when and how to employ AI tools. Given these requirements, an AI-ready workforce must include a solid nucleus of AI*

[239] *First Quarter Recommendations*, NSCAI at 30-31 (Mar. 2020), https://www.nscai.gov/reports.

> *technical experts and developers. But the bulk of the workforce will be people who enable, or are enabled by, the effective use of AI. This larger group needs to understand the fundamentals of AI policy, functionality, and application. Accordingly, for [the Department of Defense (DOD)] and many intelligence agencies, familiarity with AI should be more widespread, from senior leaders to mid-level officials to technical staff.*[240]

To better understand the workforce, NSCAI, in partnership with the Defense Innovation Board (DIB) and Joint Artificial Intelligence Center (JAIC), developed a workforce model that frames the United States Government's AI workforce challenges. In the intervening months, as NSCAI shifted from problem framing to developing solutions, focus transitioned to the five categories discussed below. These categories best describe the types of expertise the government AI workforce needs and more closely resemble common terminology in use in industry and government. It is worth noting that these are broad, generally applicable categories, and are not tied to specific parts of the government. Most departments and agencies will have a technical workforce, all have organizational and junior leaders, and many will have policy experts.[241]

- **Technical Workforce.** The technical workforce consists of the people who actively participate in the creation of AI solutions. An organization's technical expertise can be tiered, differentiating data collection, management, and software maintenance skill sets from less common and more demanding tasks such as research, algorithm development or testing, evaluation, verification, and validation (TEVV). Similarly, the skills needed to operationalize and implement differ from those needed for research and development.[242]

  Digital expertise, like any honed and sought-after trade, must be practiced consistently to maintain proficiency. Digital subject matter experts' frequent struggle to spend a career serving in digital roles in government is arguably the single most important issue impeding government modernization.[243] The DoD, for example, treats digital competency among its servicemembers as a supplementary skill, practiced intermittently and rarely used as a key driver in making assignments. This results in a system that does not leverage the critical skills of its existing workforce, instead creating additional challenges for the recruitment of technical experts.[244]

  To truly become an AI-enabled organization, the government will need a diverse array of technical expertise. This Tab will make several recommendations about career fields for a technical workforce, but they should not be interpreted as a comprehensive list of the technical roles needed to fully leverage AI. Instead, they should serve as a starting point to allow government agencies to begin experimenting and collecting data about their more specific technical workforce needs.

[240] *Interim Report*, NSCAI at 36 (Nov. 2019), https://www.nscai.gov/reports.
[241] Id. at 61-65. NSCAI staff have conducted more than 100 interviews with government, private-sector, and academic experts on this topic.
[242] NSCAI staff interview with a government official (Apr. 3, 2020). The skills needed parallel those in the Key Considerations for Responsible Development of AI Systems. See *Second Quarter Recommendations,* NSCAI at 93-155 (July 2020), https://www.nscai.gov/reports.
[243] NSCAI staff conversation with government and private-sector senior leaders and digital modernization experts (May 6, 2020).
[244] J. Michael McQuade, et al., *Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, Defense Innovation Board at viii (May 3, 2019), https://media.defense.gov/2019/Mar/26/2002105909/-1/-1/0/SWAP.REPORT_MAIN.BODY.3.21.19.PDF.

- **Organizational Leaders.** Organizational leaders create strategic and enterprise objectives, make resource decisions, oversee the deployment and scaling of new systems, and support the careers of their employees, including the technical workforce. As organizations switch from individual projects to enterprise AI, leaders incorporate

  AI-related tasks into their organizations' priorities, and establish and reinforce processes that enable AI. Organizational leaders who do not sufficiently understand digital technology and AI are susceptible to pursuing programs that will not add value, and failing to effectively incorporate AI into operational concepts or organizational processes. These leaders also struggle to perform effective internal oversight, and request AI solutions without prioritizing the data collection, management, processing, and responsible development practices required to make machine learning solutions helpful.[245]

- **Junior Leaders.** Junior leaders work with and directly manage end users. They serve as domain knowledge experts, interact with the technical workforce, and are a key node in feedback loops between end users and the components of the technical workforce that are building and refining AI solutions. Junior leaders with insufficient understanding of AI will struggle to responsibly field AI-enabled capabilities. Just as importantly, in a competitive environment, they will struggle to use AI to its full potential, or understand how to compete against an adversary attempting to do the same.

- **Policy Experts.** Policy experts are those who inform organization, national, and international policies. They do not lead organizations or develop AI solutions, but require enough knowledge of both AI and their domain to develop effective policies. These include some government civilians in organizations such as the Office of the Under Secretary of Defense for Policy, and perhaps most critically, diplomats in the Department of State. Notably, this group was not addressed in the Commission's *2019 Interim Report Appendix 3: Workforce Model*,[246] but research since then has shown that policy experts are a distinct and important group. Policy experts who do not understand AI well enough struggle to negotiate effectively with allies and adversaries once the subject matter moves beyond basic AI topics and into discussions that require some technical knowledge.[247] To avoid this problem, policy experts need to understand both policy and technology, but do not need to be engineers.

- **Acquisition Professionals.** Acquisition professionals are responsible for managing and executing the procurement and sustainment of AI software and services. One of the most common themes heard during NSCAI's interviews is that acquisition professionals lack familiarity with software and AI, presenting a major hurdle for organizations that want to acquire the resources to adopt AI solutions. Even the few organizations that have aggressively educated their leaders and

[245] NSCAI staff interview with several government officials (May 24, 2019); NSCAI staff interview with a government official (May 5, 2020). These problems stem from unrealistic expectations of AI's capabilities, a poor understanding of most machine learning solutions' data requirements, and from not understanding that most AI projects, even in successful companies, fail.
[246] *Interim Report*, NSCAI at 61-65 (Nov. 2019), https://www.nscai.gov/reports.
[247] NSCAI staff interview with a former government official (Apr. 24, 2020).

> recruited a technical workforce have struggled to educate and recruit acquisition professionals able to effectively acquire AI software and services.[248] Our military and government leaders have too often dealt with poor information technology, massive acquisition failures, and sub-par analysis that results in major national security risks.[249] Poor acquisition decisions have likely caused more damage to the military than budget cuts.[250] Another provided that acquisition professionals should begin to think about AI as a capability ecosystem (resources, process, technology, data, and governance) as opposed to simply AI "widgets" that are procured separately. Ultimately, our acquisition professionals must possess the requisite skills and knowledge to effectively and efficiently procure both software and hardware, including AI solutions, and must understand how to do so across all phases of design, development, deployment, sustainment, and disposal.

Issue 1: Existing Initiatives within the Military Services

The United States Government already has several promising AI, data science, and software development workforce initiatives either planned or in the early phases of implementation.[251] While many of these programs do not focus solely on AI, they all address technologies needed to enable AI, such as data management, electrical engineering, and software. This aligns with judgement 13 from the *NSCAI 2019 Interim Report*:

> *National security agencies need to rethink the requirements for an AI-ready workforce. That includes extending familiarity with a range of relevant AI technologies throughout organizations, infusing training on the ethical and responsible development and fielding of AI at every level, and spreading the use of modern software tools*.[252]

It also aligns with judgement 14, that the:

> *DoD and the* [*Intelligence Community (IC)*] *are failing to capitalize on existing technical talent because they do not have effective ways to identify AI-relevant skills already present in their workforce. They should systematically measure and incentivize the development of those skills.*[253]

In general, the military services and government agencies should train and educate their end users and junior leaders to use AI-enabled systems, including the specific topics mentioned in Issue 6 below. The training and education programs should also address related topics and technologies, including but not limited to software development, data science, electrical

[248] NSCAI staff interview with a government official (May 8, 2020).
[249] See e.g., *High Risk Series: Substantial Efforts Needed to Achieve Greater Progress in High-Risk Areas*, United States Government Accountability Office at 123 (Mar. 2019), https://www.gao.gov/assets/700/697245.pdf (". . . federal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes").
[250] Id. at 143 ("Congress and DOD have long sought to improve how major weapon systems are acquired, yet many DOD programs continue to fall short of cost, schedule, and performance goals. Consequently, DOD often pays more than anticipated, buys less than expected, and, in some cases, delivers fewer capabilities to the warfighter.").
[251] A recommendation regarding the Marine Corps is not listed in this section because, at the time of writing, their AI and data science workforce strategy is still in draft form.
[252] *Interim Report*, NSCAI at 36 (Nov. 2019), https://www.nscai.gov/reports.
[253] Id. at 37.

engineering, and computer science. The military services and government agencies should also enroll senior leaders in executive education programs that address the basics of AI, organizational transformation, and related topics.

Recommendation 1.1: Support the Army AI Task Force's AI and Data Science Workforce Initiative

The U.S. Army has an ambitious AI and data science workforce initiative. The U.S. Army AI Task Force partners with the Carnegie Mellon University (CMU), and has begun a four-pronged training and education program.

- **Executive Education.** The U.S. Army initiated an executive education program that will include all two and three star commanders, select members of their staff, and select Senior Executive Service (SES) personnel. The course will consist of five sessions, the first and last of which will be two to three days in-residence. The middle three sessions will be via distance learning. The education will be project-based, focused on data leadership, and on producing leaders that can drive AI modernization by focusing on socio-technical change rather than just technical change.[254]

- **AI Professionals.** AI professionals are roughly equivalent to AI experts and AI developers in the NSCAI workforce model.[255] Approximately 24 AI professionals will begin attending master's degree programs in data science and analytics or data engineering at CMU in the fall semester of 2020. The program plans to expand to other universities. Uniformed graduates will temporarily or permanently serve as Functional Area (FA) 49 (Operational Research and Systems Analysis) or FA26 (Information Network Engineering) officers. Notably, these are not AI or data science specific functional areas or career fields (which do not exist), and it has not been determined that uniformed personnel would be able to continue serving in those roles rather than moving back to their original branch, e.g. infantry.[256]

- **Technicians.** Beginning this year, 12 enlisted personnel will attend a one-year fellowship at CMU that includes a 14-week course focused on data science and analytics. After completing the fellowship, they will return to the operational force to train AI users.

- **AI Users.** Each technician will be expected to train roughly 100 AI users a year at installations across the U.S. Army. The program's goal is to train 400,000 AI users over roughly the next ten years.[257]

[254] NSCAI staff interview with a government official (April 3, 2020).

[255] *Interim Report*, NSCAI at 61-65 (Nov. 2019), https://www.nscai.gov/reports.

[256] NSCAI staff interview with a government official (April 3, 2020). NSCAI also addresses the need to create career fields that will allow uniformed personnel to spend a career focused on digital skills in Issue #4 of this report.

[257] Id.

Proposed Legislative Branch Action

The Armed Services Committees sustain support for the U.S. Army AI Task Force's AI workforce initiative. The Commission recommends appropriators set aside $5,000,000 of Army Operations & Maintenance (O&M) appropriations funding in Fiscal Year (FY) 2022, and $6,000,000 in FY 2023 and subsequent years, for the U.S. Army AI Task Force's AI and data science workforce initiative to allow the U.S. Army to continue to educate its senior leaders, begin building its technical workforce, and educate a significant portion of its end users.

Recommendation 1.2: Support the Navy Community College

The U.S. Navy's Education for Seapower Strategy 2020 announced the formation of the U.S. Naval Community College (NCC).[258] The NCC will provide sophisticated and technology-focused education for enlisted sailors, Marines, and Coast Guardsmen.[259] Partnered universities will teach approximately 95 percent of courses and grant associate's and bachelor's degrees.[260] The NCC will cover 100 percent of the cost of attendance instead of asking service members to use tuition assistance, and will focus on 10 to 12 technical degrees to educate the enlisted force in the areas of complex data analysis, network engineering, and programming.[261] The U.S. Navy intends to sustain enrollment at 40,000 personnel, with 100 percent of instruction online.[262] Participation will be incentivized by a new set of metrics involving education in performance evaluations and by requiring a degree from the NCC for some positions.[263] The U.S. Navy also plans to begin distance learning graduate education in Naval Studies with several concentrations, one of which will focus on emerging technologies, and to increase the number of low-residency graduate degrees naval officers earn.[264]

Proposed Legislative Branch Action

The Armed Services Committees should sustain support for the U.S. Naval Community College.[265]

Recommendation 1.3: Support the Air Force Digital University

The U.S. Air Force includes AI as a subset of its digital literacy initiatives. The goal of the Digital University is to identify and grow digital skills including AI within the U.S. Air Force.[266] Digital University studies would center on commercial digital education and training through massive, open, online courses or in-residence programs through university partnerships.[267]

[258] NSCAI staff interview with a government official (May 5, 2020); see also *Navy's New Education for Seapower Report*, USNI News (Feb. 12, 2019), https://news.usni.org/2019/02/12/navys-new-education-seapower-report.
[259] NSCAI staff interview with a government official (May 5, 2020).
[260] Id.
[261] Id.
[262] Id.
[263] Id.
[264] Id.
[265] A proposed budget was not available from the Navy Community College.
[266] NSCAI staff interview with a government official (April 21, 2020).
[267] Id.

Proposed Legislative Branch Action

The Armed Services Committees should sustain support for the U.S. Air Force Digital University. The Commission recommends House and Senate appropriators set aside $10 million in U.S. Air Force O&M funding for the U.S. Air Force Digital University in order to allow the U.S. Air Force to significantly expand the portion of its workforce with digital skills.

Recommendation 1.4: Support the Air Force Computer Language Initiative

The U.S. Air Force includes AI as a subset of its digital literacy initiatives. The Computer Language Initiative (CLI) is a force development program that assesses digital aptitude, and provides online and in-residence training for top performers; completion of the program would result in a certificate, assignment opportunities, and a possible pay increase.[268] The CLI has been approved by senior U.S. Air Force leadership for inclusion in the FY 2022 budget, but has not been finalized yet for inclusion in the Program Objective Memorandum (POM).[269]

Proposed Legislative Branch Action

The Armed Services Committees should sustain support for the CLI. The Commission recommends appropriators set aside $10 million in U.S. Air Force O&M funding for the CLI in order to increase the portion of the U.S. Air Force able to code in relevant software languages.

Recommendation 1.5: Support the U.S. Air Force/Massachusetts Institute of Technology (MIT) AI Accelerator

The U.S. Air Force/MIT AI Accelerator is the first operational Air Force AI unit and is co-located at MIT.[270] The AI Accelerator has both officer and enlisted Airmen from seven career fields developing, training, and transitioning AI into operations.[271] It is a clearinghouse for AI workforce initiatives. Airmen are matched with MIT and MIT Lincoln laboratory staff and put through an apprenticeship where they learn how to develop, test, and deploy AI systems across 10 separate AI applications.[272] This model has led to the field testing of AI optimization algorithms of Mission Scheduling/Planning in less than four months. The U.S. Air Force/MIT AI Accelerator has been approved by senior Air Force leadership for inclusion in the FY 2022 POM, but full funding has not been finalized for the FY 2021 budget.[273]

Proposed Legislative Branch Action

The Armed Services Committees should sustain support for the U.S. Air Force/MIT AI Accelerator. The Commission recommends appropriators set aside $15 million in Air Force

[268] Id.
[269] Id.
[270] NSCAI staff interview with a government official (July 1, 2020).
[271] Id.
[272] Id.
[273] Id.

research & development (R&D) funding for FY 2021 in order to accelerate the U.S. Air Force's ability to adopt AI both by improving the technology it has access to and training its workforce to build and use it.

Issue 2: Managing Civilian Subject Matter Experts

United States Government civilians play a critical role in the national security enterprise. Far from being administrative continuity, a significant portion of the government's AI talent is likely to exist in the civilian workforce. If the United States Government does not invest in managing and developing its civilian digital workforce, it will struggle to create the cadre of experts it needs.

Unfortunately, United States Government civilians currently do not have career paths outside of research and development that allow them to focus on software development, data science, or AI for the majority of their career. This results in a highly limited ability to recruit talent from outside of government, an inability for an individual to focus on a skill set for an extended time, a lack of continuing education opportunities for these government civilians, and retention issues. It also causes the government to struggle to identify and manage the software development, data science, and AI talent within its workforce.[274]

As noted in the introduction, digital subject matter experts' inability to spend a career working on digital topics while serving in government is arguably the single most important issue impeding government modernization.[275] A digitally focused occupational series will better allow the government to track and manage its digital workforce, to attract new talent that wants to focus on a technical skill set, and to create new positions. While creating occupational series will make it easier for agencies to create digital positions, it will not, alone, create billets for digital experts to fill. Creating these billets requires a demand signal from leaders. It is also worth noting that experts need to access modern software tools to perform their jobs effectively. If they are denied access to these tools, many experts will leave the government. While this is not directly a talent management issue, it will have a major impact on the government's ability to recruit and retain experts.

This aligns with judgement 13 from the *2019 Interim Report*:

> *National security agencies need to rethink the requirements for an AI-ready workforce. That includes extending familiarity with a range of relevant AI technologies throughout organizations, infusing training on the ethical and responsible development and fielding of AI at every level, and spreading the use of modern software tools*.[276]

[274] This analysis is based on the NSCAI staff conducting more than 100 interviews with government officials between May 2019 and May 2020. This feedback has emerged as a common theme in nearly all of NSCAI's workforce discussions. See e.g., NSCAI interviews with government officials (June 7, 2019); NSCAI interviews with government officials (May 17, 2019).

[275] NSCAI staff conversation with government and private-sector senior leaders (May 6, 2020).

[276] *Interim Report*, NSCAI at 36 (Nov. 2019), https://www.nscai.gov/reports.

It also aligns with judgement 14, that the:

> *DOD and IC are failing to capitalize on existing technical talent because they do not have effective ways to identify AI-relevant skills already present in their workforce. They should systematically measure and incentivize the development of those skills.*[277]

Further, it also aligns with judgement 17, that:

> *The military and national security agencies are struggling to compete for top AI talent. They need a better pitch, incentive structure, and better on-ramps for recent graduates.*[278]

The Office of Personnel Management (OPM) follows a three-phase process to create a new occupational series.[279] During the first step, a department's or agency's Chief Human Capital Officer must submit a formal request to OPM to create a new occupational series. The request includes: 1) the current classification of covered positions, 2) the number of covered positions, 3) an explanation of why the current classification is not effective, 4) any supporting documentation, 5) the position's duties and responsibilities, and 6) the position's government-wide impact. During the second phase, OPM determines if the request is substantiated. If determined to be substantiated, OPM moves to phase three.

During phase three, OPM requests any other supporting documents needed from the relevant agency or agencies, and the lead agencies work with OPM to provide subject matter experts for the remainder of the process. OPM then drafts a classification policy and issues the policy for comment to agency human resource directors and the public for 60 days. Once the 60-day period is complete, OPM edits and revises the policy, and releases it for implementation.

The described process is necessarily rigorous, but it can be done in six to 12 months. Unfortunately, despite its potential speed, it sometimes takes much longer. The above system relies on Chief Human Capital Officers' identification of quantifiable deficits in the workforce.[280] This relies on the identification of a new need, and an analysis of the number and type of personnel needed to perform a known task. While this is adequate for some tasks, it is poorly suited for AI. AI and some other emerging technologies will create new capabilities and processes. Offices performing gap analysis struggle to measure workforce deficits related to tasks the government has not yet performed.

Recommendation 1.6: Accelerate Existing Occupational Series Initiatives

The DoD is researching software development and software engineering occupational series, and OPM is considering creating knowledge management and data science occupational series. The government should create software development, software engineering, data science, and knowledge management occupational series. This combination of occupational

[277] Id. at 37.

[278] Id. at 38.

[279] NSCAI staff interview with a government official (Oct. 8, 2019).

[280] NSCAI staff interview with a government official (June 21, 2019); NSCAI staff interview with a government official (June 24, 2019); NSCAI staff interview with a government official (July 16, 2019); NSCAI staff interview with a government official (July 25, 2019).

series would significantly improve the government's ability to recruit and manage experts that will supervise the collection and curation of data, build human-machine interfaces, and help end users generate and act on data-informed insights. Many successful private-sector organizations use a version of this combination of skills.[281] The government should follow their example.

Proposed Executive Branch Action

OPM should create software development, software engineering, data science, and knowledge management occupational series. Rather than waiting for agencies to provide a formal request for a new occupational series, OPM should move to phase three, and ask agencies to provide supporting documents and subject matter experts to study and draft a classification policy for each occupational series.

Proposed Legislative Branch Action

The Congress should enact legislation to require OPM to draft software development, software engineering, data science, and knowledge management occupational series classification policies no later than 270 days after the passage of the legislation.

Recommendation 1.7: Create an AI Occupational Series

While the above-listed occupational series will contribute significantly to the United States Government's digital modernization, they do not adequately address the full scope of the civilian AI workforce the United States Government will need, which will include project managers, cloud computing application architects, machine learning engineers, user-experience researchers, ethicists, and other roles.[282] The United States Government should explore the need to establish these fields by creating an AI occupational series, then adding parenthetical titles as needed to identify more specialized requirements as needed.[283]

Proposed Executive Branch Action

OPM should create an AI occupational series. Rather than waiting for agencies to provide a formal request for a new occupational series, OPM should move to phase three, and ask agencies to provide supporting documents and subject matter experts to study and draft a classification policy for each occupational series.

Proposed Legislative Branch Action

The Congress should pass legislation to require OPM to draft a classification policy for an AI occupational series no later than 270 days after the passage of the legislation.

[281] NSCAI staff interview with a private-sector company (Sept. 9, 2019); NSCAI staff interview with a private-sector company (Sept. 19, 2019); NSCAI staff interview with a private-sector company (Apr. 24, 2020).
[282] *Interim Report*, NSCAI at 63 (Nov. 2019), https://www.nscai.gov/reports.
[283] *Introduction to the Position Classification Standards: TS-134*, U.S. Office of Personnel Management at 15 (Aug. 2009), https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/positionclassificationintro.pdf.

Issue 3: Recruiting Civilian Subject Matter Experts

The United States Government needs to improve and increase its recruitment of civilian subject matter experts. As noted above, the government needs an AI workforce with enough experts to identify opportunities, acquire AI solutions, and build them when necessary. While the uniformed services justifiably spend hundreds of millions of dollars on recruitment bonuses,[284] the United States Government dedicates relatively little time, money, or consolidated effort towards recruiting its civilian workforce. Unsurprisingly, this contributes to the government's struggle to build its science, technology, engineering, and mathematics (STEM) workforce. NSCAI's *First Quarter Recommendations*, if implemented, would streamline and accelerate the hiring process and allow well-qualified AI practitioners to bypass regulatory roadblocks. While these are important first steps, they will not address the need for the government to hire a large number of technologists. This aligns with *NSCAI 2019 Interim Report* judgement 15, that:

> *The United States Government is not fully utilizing civilian hiring authorities to recruit AI talent. Agencies need to make better use of pipelines for people with STEM training.*[285]

It also aligns with judgement 17, that:

> *The military and national security agencies are struggling to compete for top AI talent. They need a better pitch, incentive structure, and better on-ramps for recent graduates.*[286]

Existing programs recruit some civilian subject matter experts, though none of these programs focus on AI or AI-related fields.[287] The DoD has some STEM focused scholarship programs such as Science Mathematics, and Research for Transformation (SMART) Defense Scholarship: Scholarship-For-Service, which awarded 382 scholarships in FY 2018 and 298 scholarships in FY 2019.[288] Proposed STEM Corps legislation would aim to recruit approximately 500 recent graduates per year to the DoD.[289] It is realistic to expect that if the STEM Corps proposal is enacted, the programs together will recruit between 800 and 900 recent graduates into the DoD each year, most of whom would serve for two to three years. CyberCorps: Scholarship for Service, which graduated 307 students in FY 2019, is projected to graduate 380 students in FY 2020 for non-DoD agencies, but as of this publication it focuses only on cyber related skills and does not cover AI.[290] The United States Digital Service Academy,[291] if created by Congress, will produce approximately 500 digital subject matter experts a year that could work at any federal agency. The FY 2020 National Defense

[284] Meghann Myers, *To Draw More Soldiers, the Army Wants More Recruiters, Bigger Budgets and a Better Slogan*, ArmyTimes (Nov. 7, 2018), https://www.armytimes.com/news/your-army/2018/11/07/to-draw-more-soldiers-the-army-wants-more-recruiters-bigger-budgets-and-a-better-slogan/.

[285] *Interim Report*, NSCAI at 37 (Nov. 2019), https://www.nscai.gov/reports.

[286] Id. at 38.

[287] AI related fields include applied mathematics, statistics, operations research, electrical engineering, and computer science.

[288] *Award Statistics*, SMART (last accessed Sept. 24, 2020), https://smartscholarshipprod.servicenowservices.com/smart?id=kb_article&sys_id=07f6d2dcdba0b7000155f3421f9619aa.

[289] The STEM Corps proposal has funding for approximately 110 scholarships, but plans to use public-private partnerships to increase the funding available to enough for 500 scholarships.

[290] NSCAI staff interview with a government official (March 9, 2020).

[291] NSCAI recommended the creation of the United States Digital Service Academy in its *Second Quarter Recommendations*. See *Second Quarter Recommendations*, NSCAI at 43 (July 2020), https://www.nscai.gov/reports.

Authorization Act (NDAA)[292] includes authorization for a Defense Civilian Training Corps that will train civilians for service in the DoD. The bill authorizes DoD to establish the program at 20 schools and to enroll 400 students by 2023.[293]

Overall, there are two notable deficits. The first is a lack of AI focused recruitment. None of the programs—even those with broad STEM agendas—focus on recruiting graduates with AI oriented educations. The second flaw is that non-DoD agencies do not have a recruitment mechanism for recruiting STEM or digital talent outside of cyber fields. While the United States Digital Service Academy recommended for adoption in our *Second Quarter Recommendations* is expected to address this issue, it is unlikely to produce graduates before 2028, even if authorized and funded expeditiously. Notably, recommendations 8, 9, 10, and 11 could each be connected to or be subordinate to agency-level digital corps.

Recommendation 1.8: Enact the STEM Corps Proposal

A bipartisan group of members of the House Armed Services Committee have proposed H.R. 6526, STEM Corps Act of 2020. The proposal would authorize the appropriation of $5 million per fiscal year, with $500,000 for administrative costs and an advisory board.[294] The program provides a maximum scholarship of $40,000 per student per year. Scholarship recipients would serve in different capacities within the DoD for a minimum of three years, with an option to either remain in the DoD or transfer to a private-sector company that has contributed to STEM Corps funding. The proposal requires participants to be paid at a rate not less than GS-6 for the first three years of their obligation and at not less than as a GS-10 during their fourth year.[295] This proposal has the potential to significantly increase the number of personnel with STEM backgrounds in the DoD civilian workforce for a relatively low cost if a sufficient number of private-sector companies contribute. The potential for recipients to transfer to the private sector after three years of government service may create retention issues, but it may also serve as a mechanism to create bridges between the DoD and private sector companies.

Proposed Legislative Branch Action

The Armed Services Committees should include the proposal to establish a STEM Corps in the FY 2022 NDAA. Appropriators should set aside $5 million for a STEM Corps for FY 2022 and each fiscal year thereafter.

Proposed Executive Branch Action

The DoD should, with congressional authorization and appropriation, establish an office to manage and establish a STEM Corps as described above and in the STEM Corps proposed legislation, including a scholarship program, advisory board, private-sector partnership program, and STEM Corps member management program.

[292] Pub. Law 116-92, National Defense Authorization Act for Fiscal Year 2020 at § 860 (2019).
[293] Id.
[294] H.R. 6526, STEM Corps Act of 2020 at 7 (introduced Apr. 17, 2020).
[295] Id. at 10-11.

Recommendation 1.9: Endorse an AI Scholarship for Service Proposal

NSCAI *First Quarter Recommendation*s included a proposal to expand CyberCorps: Scholarship for Service (SFS) to include digital engineering.[296] While the Commission believes that is a valuable proposal, the Commission also believes there is a need to establish an AI Scholarship for Service program that more directly recruits students studying AI and AI related fields. Such a program would increase the number of AI focused recent graduates serving in government, and would be more responsive to the government's AI requirements than SFS programs that are responsible for recruiting students studying cyber topics or STEM in general.[297]

Proposed Legislative Branch Action

The appropriate committees should include a proposal to establish an Artificial Intelligence Scholarship for Service program in the FY 2022 NDAA. This program should closely reflect the Cybersecurity Enhancement Act of 2014, as amended by the FY 2018 NDAA.[298]

Proposed Executive Branch Action

Once authorized by Congress, the National Science Foundation (NSF), in coordination with the Office of Personnel Management, should establish an AI Scholarship for Service program modeled after CyberCorps: Scholarship for Service. This should include establishing criteria for AI centers of excellence, tuition, stipends, and a service obligation.

Recommendation 1.10: Create Digital Talent Recruiting Offices

While scholarship for service programs play a valuable role, they are not designed to efficiently meet specific agencies' digital workforce recruitment needs. This is problematic, as the government needs to quickly increase the size and capabilities of its digital workforce. Executive Branch agencies should create agency level digital talent offices of up to 20 personnel responsible for recruiting both early career and experienced professionals. Recruiting offices would monitor their agencies' need for specific types of digital talent. The offices would be empowered to recruit technologists virtually, by attending conferences, career fairs, recruiting on college campuses, and offering scholarships, recruiting bonuses, referral bonuses, non-traditional recruiting techniques such as prize competitions, and other recruiting mechanisms. A recruiting office would assume responsibility for their agency's digital talent recruitment efforts, e.g. SMART: SFS, and partner with agency human resources offices to use direct-hire authorities to accelerate hiring. This would help scale digital talent recruitment by creating a central, empowered organization that focuses on a specific mission; concentrates expertise and funds; would help experts move in and out of government positions throughout their career; and can develop relationships with universities and private-sector companies.

[296] *First Quarter Recommendations*, NSCAI at 39-40 (Mar. 2020), https://www.nscai.gov/reports.
[297] The AI Scholarship-for-Service Act (S. 3901) introduced by Senators Peters and Gardner would achieve the goal of this recommendation.
[298] Pub. L. 113-274, sec. 302, Cybersecurity Enhancement Act of 2014, 128 Stat. 2971; Pub. L. 115-91, sec. 1649b, The National Defense Authorization Act for Fiscal Year 2018, 131 Stat. 1283 (2017).

Proposed Legislative Branch Action

The Armed Services Committees should amend section 230 of the FY 2020 NDAA to require the DoD to appoint a civilian official responsible for digital engineering talent recruitment policies and their implementation. The civilian official should be supported by a digital talent recruiting office with the Office of the Undersecretary for Personnel and Readiness, as described above.

The Intelligence Committees should require the Office of the Director of National Intelligence (ODNI) to create a digital talent recruiting office that works with the IC to identify their agencies' needs for specific types of digital talent; recruit technologists by attending conferences, career fairs, and actively recruiting on college campuses; integrate federal scholarship for service programs into agency recruiting; offer recruitment and referral bonuses; and, partner with their agencies' human resource teams to use direct-hire authorities to accelerate hiring.

The Senate Homeland Security and Governmental Affairs Committee and the House Committee on Homeland Security should require the Department of Homeland Security (DHS) to create a digital talent recruiting office that works with the IC to identify their agencies' needs for specific types of digital talent; recruit technologists by attending conferences, career fairs, and actively recruiting on college campuses; integrate federal scholarship for service programs into agency recruiting; offer recruitment and referral bonuses; and partner with their agencies' human resource teams to use direct-hire authorities to accelerate hiring.

The Senate Committee on Energy and Natural Resources and the House Committee on Energy and Commerce should require the Department of Energy (DoE) to create a digital talent recruiting office that works with the DoE to identify its needs for specific types of digital talent; recruit technologists by attending conferences, career fairs, and actively recruiting on college campuses; integrate federal scholarship for service programs into agency recruiting; offer recruitment and referral bonuses; and partner with their agencies' human resource teams to use direct-hire authorities to accelerate hiring.

Proposed Executive Branch Action

The DoD (including U.S. military services), DOE, DHS, and the ODNI should create digital talent recruiting offices that monitor their agencies' need for specific types of digital talent; recruit technologists by attending conferences, career fairs, and actively recruiting on college campuses; integrate federal scholarship for service programs into agency recruiting; offer recruitment and referral bonuses; and partner with their agencies' human resource teams to use direct-hire authorities to accelerate hiring.

Recommendation 1.11: Establish a public-private talent exchange (PPTE) program at non-DoD national security agencies

The current federal workforce is limited by the number of available AI practitioners and proficient technology practitioners. Additionally, it is difficult for government employees to stay current on the latest commercial state of practice or the innovative techniques found in the commercial sector. As the Commission has previously found, the Federal Government needs new pathways to onboard AI talent. And, while there are some existing programs that allow national security departments and agencies to augment their workforce through talent exchanges, those existing programs are primarily targeted towards the DoD and narrowly focused on areas such as information technology and cybersecurity.[299]

The Intergovernmental Personnel Act (IPA) allows for personnel exchanges between the Federal Government and state, local, or tribal governments, academia, or national laboratories.[300] The IPA mechanism is a powerful tool, with the potential to enable national security agencies to significantly augment their workforces with AI experts. Unfortunately, in large parts of the DoD, the IPA mechanism is an underutilized tool, and often takes far too long to approve when it is used. Agencies, especially the DoD, should place greater emphasis on recruiting external talent through IPAs, and fast tracking the IPA approval process whenever possible.

While helpful for other parts of the government, academia, and national laboratories, IPA was not designed to exchange talent with the commercial sector. Within the commercial sector, there exists a desire to assist the government in solving complex technical problems, including a desire by commercial sector employees to temporarily serve a detail with the Federal Government. However, there are few pathways to do so for non-DoD national security departments and agencies.

Congress provided the DoD with a unique PPTE program.[301] While this pilot program is new and has not yet been determined to be successful, the Commission enthusiastically endorses establishing a similar program for other national security agencies should this program show success. Mirroring this program for other national security departments and agencies would enable them to conduct public-private talent exchanges with all of the safeguards[302] already required in the DoD's program.

[299] See e.g., Pub. Law 114-328, §1123 (2016) (authorizing the Cybersecurity Information Technology Exchange Program (CITEP)); 10 U.S.C. §1599g (regarding the Department of Defense Public-Private Talent Exchange (PPTE) program).

[300] *Policy, Data, Oversight: Hiring Information*, Office of Personnel Management (last accessed Sept. 11, 2020), https://www.opm.gov/policy-data-oversight/hiring-information/intergovernment-personnel-act/#url=Provisions.
The full list of eligible organizations include: "(1) A national, regional, Statewide, area wide, or metropolitan organization representing member State or local governments; (2) An association of State or local public officials; (3) A nonprofit organization which offers, as one of its principal functions, professional advisory, research, educational, or development services, or related services, to governments or universities concerned with public management; or (4) A federally funded research and development center." 5 U.S.C. § 3371(4).

[301] *Department Of Defense Public-Private Talent Exchange (PPTE) Program: Questions/Answers*, Defense Civilian Personnel Advisory Service, (Aug. 23, 2018), https://www.dcpas.osd.mil/Content/Documents/PPTEQuestions_Answers23Aug2018.pdf.

[302] Id. at 2 ("DoD employees must complete either a Confidential or Public Financial Disclosure Report, whichever applies; a continued service obligation agreement; ethics training in accordance with the Office of Government Ethics regulations; and all other applicable training requirements prior to the implementation of the MOA. Private-sector participants must complete either a Confidential or Public Financial Disclosure Report, whichever applies; a disqualification statement prohibiting the private-sector employee from working on matters related to his or her private-sector organization; and ethics training in accordance with Office of Government Ethics regulations prior to the implementation of the MOA.")

Proposed Executive Branch Action

The President should authorize national security departments and agencies to use any available means to expedite the fielding and application of artificial intelligence applications development and deployment, including the use of public-private talent exchanges.

Proposed Legislative Branch Action

Relevant Congressional committees should consider establishing a PPTE program for the Departments of Homeland Security, State, Energy, Commerce, Treasury, and the IC. The Commission supports the PPTE program for the IC found in Section 306 of the House's Intelligence Authorization bill.[303]

Issue 4: Managing Military Subject Matter Experts

Much like their civilian counterparts, U.S. military personnel do not have career paths that allow them to focus on software development, data science, or AI for the majority of their career.[304] The military has established career fields for doctors and lawyers that allow them to focus on a technical field, develop their skill over time, and advance within their service. The military is choosing not to do the same for many types of digital talent. While some of the services train some operational research and systems analysis (ORSA) personnel to perform machine learning and AI tasks, these personnel may be shifted to work on other ORSA tasks rather than AI. Phrased differently, AI practitioners have some background in ORSA, but not all ORSA personnel are trained to work in machine learning or AI.[305]

This results in a reduced ability to recruit talent outside of the United States Government, an inability to focus on a skill set for an extended time, a lack of continuing education opportunities, and retention issues. It also causes the government to struggle to identify and manage the software development, data science, and AI talent within its workforce.[306] Much like in the civilian workforce, digital subject matter experts' inability to spend a career working on digital topics while serving in the military is arguably the single most important issue impeding military modernization.[307] These problems are particularly acute for military personnel, who are required to regularly change positions and move into manager roles or face eventual discharge from the military. The lack of digital career fields also causes the military services to struggle to identify and manage the software development, data science,

[303] H.R. 3494, Sec. 306, Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/3494/text.

[304] *Workforce Now: Responding to the Digital Readiness Crisis in Today's Military*, Defense Innovation Board at 1-7 (2019), https://media.defense.gov/2019/Oct/31/2002204196/-1/-1/0/WORKFORCE_NOW.PDF.

[305] NSCAI staff has interviewed several ORSA personnel performing AI related tasks. All agreed when asked that a separate career field for artificial intelligence or data science is needed. As shown in Issue #1, existing initiatives make some progress, but do not adequately address the lack of career fields for digital talent.

[306] The NSCAI staff has conducted more than 100 interviews with government officials between May 2019 and May 2020. This feedback has emerged as a common theme in nearly all of NSCAI's workforce discussions. See e.g., NSCAI interviews with government officials (June 7, 2019); NSCAI interviews with government officials (May 17, 2019).

[307] NSCAI staff interviews with government and private-sector senior leaders (May 6, 2020).

and AI talent within their workforces.[308] As long as this state continues, the military should not expect to achieve better results for its digital modernization than its legal and medical fields would have without career fields for lawyers and doctors.

The military services should have career fields that allow digital talent to focus on digital skills and work as a career. This does not imply that digital talent should be separated from operational roles. Instead, they serve in both garrison positions and in operational roles.[309] In the options below, occupational specialty refers to a full-time career field or branch that military service members enter at the start of their career or transfer into, and which is managed by a central authority.[310] Functional areas are areas of specialization that service members can transfer into and are independently managed. Different services also show that personnel are certified to perform specialized tasks with a marker in their personnel file. Additional Skill Identifiers (ASI), Additional Qualification Designations (AQD), Additional Military Occupational Specialty (AMOS), and Special Experience Identifiers (SEI) are certifications military personnel earn, typically by attending a course, that show they are able to perform certain tasks and that are monitored by the personnel system.[311] Certain certifications or the associated training are required or highly preferred for many positions. Personnel with this type of certification are managed by their branch, not by a central organization in charge of personnel with each particular certification.

This aligns with *NSCAI 2019 Interim Report* judgement 14, that the:

> *DOD and IC are failing to capitalize on existing technical talent because they do not have effective ways to identify AI-relevant skills already present in their workforce. They should systematically measure and incentivize the development of those skills.*

It also aligns with judgement 17, that:

> *The military and national security agencies are struggling to compete for top AI talent. They need a better pitch, incentive structure, and better on-ramps for recent graduates.*[312]

Recommendation 1.12: Create New Career Fields

The military services should have primary career fields that allow military personnel to focus on software development, data science, or artificial intelligence for their entire career, either as managers or technical specialists.

[308] NSCAI's First Quarter Recommendations included an addition to the Armed Services Vocational Aptitude Battery to test for computational thinking that would help identify aptitude and a test for coding language proficiency that would help identify skill. *First Quarter Recommendations*, NSCAI at 33-35 (Mar. 2020), https://www.nscai.gov/reports. Both tests will be helpful, but will not meet their full utility without digital career fields. In conversations with NSCAI, numerous government officials continuously identified a lack of digital career fields as a key impediment to talent management. See e.g., NSCAI interviews with government officials (June 7, 2019); NSCAI interviews with government officials (May 17, 2019).

[309] Flight surgeons can serve as a model for military AI practitioners. Flight surgeons are medical professionals with technical training who serve a role in garrison, but also receive operational training and fill a specialized billet in operational units.

[310] These are referred to as military occupational specialties in the Army, primary military occupational specialties in the Marine Corps, Air Force specialty codes in the Air Force, and ratings or primary designators in the Navy.

[311] Army personnel earn ASIs, Navy personnel earn AQDs, Marine Corps personnel earn AMOS, and Air Force personnel earn SEI.

[312] *Interim Report*, NSCAI at 37 (Nov. 2019), https://www.nscai.gov/reports.

Proposed Legislative Branch Action

The Armed Services Committees should amend section 230 of the FY 2020 NDAA to require the military service chiefs to create career fields focused on software development, career fields focused on data science, and career fields focused on artificial intelligence for both commissioned officers and enlisted personnel, and, as appropriate, warrant officers. Military personnel should be able to join these career fields either upon entry into the military, or by transferring into the field after serving a period in another career field. These career fields should have options that allow personnel to either follow a path to senior leadership positions, or specialize and focus on technical skill sets. Those that specialize and focus on technical skill sets should not have to leave their focus area and move into management positions to continue to promote. Legislation should not restrict the military services to only two career fields, but rather require each service to create at least two career fields, and more at their discretion. The military services should be required to create the career fields within one year of passage of legislation.

Proposed Executive Branch Action

The military services should create career fields that allow military personnel to focus on software development, career fields that allow military personnel to focus on data science, and career fields that allow military personnel to focus on artificial intelligence. While remaining consistent with service personnel policies and procedures, these career fields should be open to both enlisted personnel and commissioned officers, and, as appropriate, warrant officers. Military personnel should be able to join these career fields either upon entry into the military, or by transferring into the field after serving a period in another career field. These career fields should have options that allow personnel to either follow a path to senior leadership positions, or specialize and focus on technical skill sets. Those that specialize and focus on technical skill sets should not have to leave their focus area and move into management positions to continue to promote.

Recommendation 1.13: Create ASI, AQD, AMOS, and SEI for Topics Related to AI

ASI, AQD, AMOS, and SEI are certifications military personnel earn, typically by completing a course, that shows they are able to perform certain tasks. As an example, soldiers receive an additional skill identifier 'P' after earning their parachutist badge, allowing them to participate in airborne operations. The personnel system can view additional skill identifiers to track and manage skill sets. Certain certifications or associated training are either required or highly preferred for many positions. Personnel with these certifications are managed by their primary branch, not by a central organization in charge of personnel with their certification. Military services should create or purchase training for certifications and continuing education in the following areas:[313]

- **AI Mission Engineering.** Brings specific domain expertise in operations, systems, and policies, and is likely a current or former systems operator; focuses on implementation, user adoption, and change management. The certifications should

[313] Recommendations based on NSCAI dialogue with industry experts. NSCAI staff interview (Apr. 24, 2020); NSCAI staff interview (May 8, 2020).

have methodological subcategories for natural language processing, machine vision, signal processing, and autonomy;

- **Data Engineering.** Shapes selection and review of training and test data sets, data management, data cleansing, and ensures training, testing, and operational data are matched to mission requirements. The certification should include methodological subcategories for natural language processing, machine vision, signal processing, and autonomy;

- **Safety and Responsible AI Engineering.** Focuses on operational metrics and risks, helps determine initial operational capability and full operational capability status, some model and mission validation and verification, supports ensuring compliance with relevant guidance for responsible AI adoption (e.g., DoD AI principles, IC AI Principles), system controls and safe deployment. The certification should include methodological subcategories for natural language processing, machine vision, signal processing, and autonomy; and

- **AI Hardware Technician.** Focuses on infrastructure installation hardware and software maintenance, service support, incident/event management, and monitors system performance.

For example, a service member could become certified in AI mission engineering for machine vision applications, but would not automatically also be certified for AI mission engineering for robotics.

Proposed Legislative Branch Action

The Armed Services Committees should use the FY 2022 NDAA to require the military services to create ASIs, AQDs, AMOS, and SEIs for mission engineering, data engineering, safety and responsible AI engineering, and AI hardware technicians, as described above. This should include a requirement to establish courses to instruct and certify that personnel can perform the above listed tasks, either by using existing private sector courses or by establishing a service or joint course.

Appropriators should set aside $30,000,000 of DoD O&M funding each year for the creation and execution of training courses for mission engineering, data engineering, safety engineering, and AI hardware engineering.

Proposed Executive Branch Action

The military services should create ASIs, AQDs, AMOS, and SEIs for mission engineering, data engineering, safety and responsible AI engineering, and AI hardware technicians, as described above. Military services should establish courses to instruct and certify that personnel can perform the above listed tasks, either by using existing private sector courses or by establishing a service or joint course. Service members that complete the course should receive a certification and appropriate authorization to operate and data access in their organization. Military services should prioritize training personnel in all warfighting functions, either through the use of mobile training teams or by prioritizing training above other training schools.

Issue 5: Junior Leader Training and Education

Ideally, the United States Government would rely on the public school and university system to produce a workforce with the math, data science, and problem-solving skills needed to work in an environment with ubiquitous AI. Unfortunately, few parts of the United States' school systems adequately teach those lessons to enough of their population, and the government cannot wait a generation for educational reform to produce an adequately educated workforce. In the interim, the government needs to seize the initiative and develop its workforce.[314] This aligns with judgement 13 from the *NSCAI 2019 Interim Report* that:

> *National security agencies need to rethink the requirements for an AI-ready workforce. That includes extending familiarity with a range of relevant AI technologies throughout organizations, infusing training on the ethical and responsible development and fielding of AI at every level, and spreading the use of modern software tools*.[315]

Junior leaders need to understand enough about AI to manage and operate AI-enabled organizations responsibly and effectively. Military leaders, especially those operating in a tactical environment, need to understand how to effectively provide input to machines, how to understand machine outputs, and critically, when to trust or not trust machine outputs. The application agnostic knowledge, skills, and abilities needed to perform those tasks are below. Some components of the workforce will also need more specific areas of focus, such as technology horizon scanning, analysis of foreign emerging technology capabilities, or application specific skills, but training for those more niche areas will be most effectively addressed by individual agencies, and will not be discussed in this section. Instead, this section will focus on the skills that most junior leaders will need to work in an organization with wide-spread AI.

The NSCAI staff conducted a literature review and interviewed developers, program managers, and organizational leaders working in the government and private sector to develop the below list. Each was asked which topics are relevant for domain-focused junior leaders regardless of application, and which application (e.g. natural language processing, machine vision) requires specific attention for all DoD, IC, or government junior leaders. No application specific topics were selected by any interviewee.

National security leaders need to understand the following topics:

- **Problem Definition and Curation.** Military leaders need to understand problem curation, or the process of discovering the causal mechanisms that lead to problems, associated issues, stakeholders, and potentially minimum viable products.[316] Poor problem definition and curation can lead to projects that attempt to solve the incorrect problem, and that result in significant amounts of wasted time

[314] NSCAI recommends addressing the government workforce's digital talent from the first time the government makes contact with a potential employee until they retire. See e.g., *First Quarter Recommendations*, NSCAI at 34 (Mar. 2020), https://www.nscai.gov/reports (including a recommendation to add computational thinking to the ASVAB, which would allow the military to identify potential digital talent prior to assigning career fields). Recommendations in this report would also add digital and emerging technology training throughout military careers.

[315] *Interim Report*, NSCAI at 36 (Nov. 2019), https://www.nscai.gov/reports.

[316] Steve Blank & Pete Newell, *What Your Innovation Process Should Look Like*, Harvard Business Review (Sept. 11, 2017), https://hbr.org/2017/09/what-your-innovation-process-should-look-like.

and money. This is particularly true regarding AI. Not all problems can be solved with AI, or with data-driven processes due to challenges collecting useful data sets, or problems that are not readily solvable using the type of probabilistic reasoning performed by many algorithms. Also, many problems with potential AI solutions can be solved with much easier, less resource intensive techniques. Effective problem curation can help military leaders ensure they are attempting to solve the correct problem, and that they are using the right general techniques to do so.

Problem curation is an iterative process that is teachable in classrooms and with project-based curriculum, such as "Hacking 4 Defense."[317] Military leaders that understand problem curation will be better able to identify problems with potential AI solutions, and, just as importantly, problems that AI will not help solve. This would not only help with the use of AI, but would also make junior leaders generally more productive.

- **A Conceptual Understanding of the AI Lifecycle.** The AI lifecycle is a model that simplifies the development and deployment of AI. It "provides a streamlined approach to visualize, plan, and prioritize strategic investments in commercial technologies and transformational research to leverage and continuously advance AI across operational domains, and achieve asymmetric capability through human augmentation and autonomous systems."[318] A conceptual understanding of the AI lifecycle would improve junior leaders' understanding of the importance of building all the capabilities needed for enterprise AI. Reinforcing the importance of building structural solutions to data collection, management, curation, installation of sensors, and other underappreciated topics would reduce organizations' attempts to create AI capabilities by adding AI at the end of a project. It will also help military leaders better understand what part of their adversaries' AI infrastructure and processes to target to degrade its effectiveness.

- **Data Collection and Management.** Junior leaders need to understand how to collect and manage data in a manner that prepares it for exploitation, and to operate in an environment where adversaries are doing the same. They also need to understand the causes, effects, and ethical implications of data bias. Poorly prepared and nonexistent data sets are a known issue that has been identified by almost every government organization interviewed by NSCAI. While bad data is a fact of life, training junior leaders to collect and manage data in the same manner, with the same degree of responsibility and technical expertise that they use for sustainment, medical care, and equipment maintenance would reduce this issue and accelerate the government's ability to create AI solutions, help inform data-informed decision making, and enable the continuous training of military systems. This is necessary for the broad adoption of AI.

- **Understanding Probabilistic Reasoning and Data Visualization.** Junior leaders need to understand enough about probabilistic reasoning and data visualization to understand the outputs of their AI systems and their implications for

[317] *Hacking for Defense*, H4D (last accessed Sept. 23, 2020), https://www.h4d.us/.
[318] Andrew Moore, el al., *The AI stack: A Blueprint for Developing and Deploying Artificial Intelligence*, Proc. SPIE 10635 (May 4, 2018), https://doi.org/10.1117/12.2309483. For a graphical depiction of the AI stack, see *About*, Carnegie Mellon University Artificial Intelligence (last accessed Sept. 23, 2020), https://ai.cs.cmu.edu/about.

a particular situation or environment. This is critically linked to understanding when to trust and not trust a system's outputs. As an example, a soldier using facial recognition or other biometric software to identify individuals during stability operations needs to understand the implications of 70 percent confidence in a positive identification versus that of 90 percent confidence. Notably, this does not require leaders to perform computational statistics, just to understand their output, a much less demanding task.

- **Data-informed Decision-making.** While all of the above will benefit leaders serving in an AI-enabled organization and improve human-machine interaction, they also culminate in data-informed decision-making. Today, many organizations rely heavily on intuitive or experience-based decision-making, often in the form of guidance from senior leaders. Data-informed, analytically based decision-making is the ability to use data to generate insights, then act on those insights. Data-driven organizations are often able to make decisions more quickly and at lower levels, and with a stronger empirical foundation than organizations that rely primarily on intuitive decision-making. This improves both the quality and the speed of decision-making.[319]

  To make data-informed decisions, leaders need to understand the nature and complexities of their problem, or how to curate problems. They need to understand how the presented data was collected, and the limitations of that process. A conceptual understanding of the AI lifecycle will provide a basic understanding how that data became an output, and a basic understanding of probability and statistics will allow them to read results in an informed manner.

  To make effective data-informed decisions, though, leaders also need to understand system thinking and critical thinking. System thinking combines all of the above to create an empirical but incomplete understanding of factors influencing a decision, and how both their system affects their AI and how their decision will affect their system. Critical thinking will help leaders understand the limits of AI, and the limits of data-informed decision-making processes that are based on imperfect information. This report references data-informed rather than data-driven decision-making because military leaders should never be bound by the imperfect information in front of them. Their critical thinking, judgement, and intuitive understanding of both their system and their environment will always have a critical role to play, even as it is informed by decision-making aids.

Recommendation 1.14: Integrating Digital Skill Sets and Computational Thinking into Military Junior Leader Education

The U.S. military already has a robust continuing education system. U.S. military personnel have a series of continuing education requirements they can meet through resident courses or distance programs. Completion of those courses is required for promotion or to fill certain billets. Course curriculum is managed by the services for most junior leader courses, and by the Joint Staff for mid-career courses.

[319] Becky Frankiewicz & Tomas Chamorro-Premuzic, *Digital Transformation Is About Talent, Not Technology*, Harvard Business Review (May 6, 2020), https://hbr.org/2020/05/digital-transformation-is-about-talent-not-technology.

The U.S. military's junior leaders need to be able to function in a world where both they and their adversaries have access to AI-enabled systems. This requires understanding problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making. U.S. military services need to update training and education requirements to introduce these topics to junior leaders.

Proposed Legislative Branch Action

The Armed Services Committees should use the FY 2022 NDAA to require the military services to integrate understanding problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making into existing, pre-commissioning or entry-level training for junior officers and training for non-commissioned officers within one year of the passage of the legislation.

Proposed Executive Branch Action

The military services need to integrate understanding problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making into pre-commissioning or entry-level training for junior officers and training for both junior and senior non-commissioned officers. The military services can accomplish this by creating new modules or courses, or by integrating this training into existing training and education for commissioned and non-commissioned officers. Whenever possible, this training should include the use of existing AI-enabled systems and tools.

Recommendation 1.15: Integrating Digital Skill Sets and Computational Thinking into Civilian Junior Leader Education

National security departments and agencies need to establish systems, practices, and resources to develop useful data sets and encourage agencies to experiment with, integrate, and scale AI projects, otherwise known as enterprise AI. While this requires technical talent, as shown in the *2019 Interim Report* workforce model, it also requires domain experts to understand enough about AI to help create, experiment with, and use AI-enabled systems.[320] The above recommendation addressed training domain experts within the uniformed military workforce. Junior leaders in the civilian workforce, however, will be equally important, and few government agencies are training or recruiting their junior leaders to perform AI-related tasks.

Civilian national security agencies should identify the components of their workforce that need to receive training, the type of training they need to receive, and how they should receive the training needed to create enterprise AI. This should include an assessment of which positions need to understand problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making. Civilian national security agencies should also identify the positions within their organizations that need to include AI-related tasks within their position description to establish enterprise AI.

[320] See *Interim Report*, NSCAI at 61-65 (Nov. 2019), https://www.nscai.gov/reports.

Proposed Legislative Branch Action

The appropriate congressional committees should require the Departments of Defense, Energy, and Homeland Security and the ODNI to deliver an assessment identifying the components of their workforce whose roles involve or will involve supporting or using AI-enabled systems, and how they should receive training about understanding problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making. Congress should also require the Departments of Defense, Energy, and Homeland Security and the ODNI to identify which positions within their organizations need to include AI-related tasks within their position description to establish enterprise AI.

Proposed Executive Branch Action

The Departments of Defense, Energy, and Homeland Security, and ODNI should identify the components of their workforce whose roles involve or will involve supporting or using AI-enabled systems, and how they should receive training about understanding problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making. The Departments of Defense, Energy, and Homeland Security, and ODNI should also identify the positions within their organizations that need to include AI-related tasks within their position description to establish enterprise AI.

Issue 6: Educating Organizational Leaders

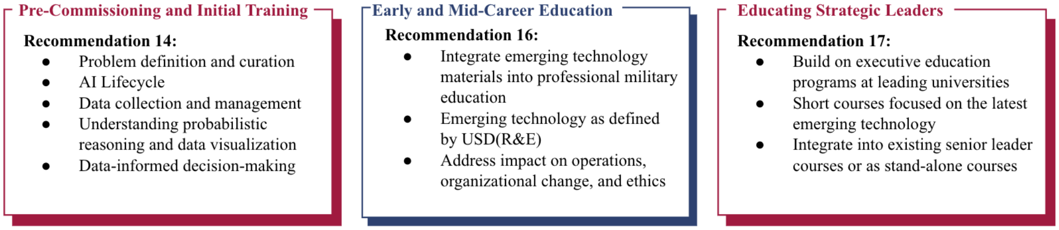
In addition to AI literacy, the government needs organizational leaders with sufficient emerging technology literacy to make informed strategic level decisions regarding the purchase or application of emerging technology and create enough of a demand signal for their organizations to prioritize emerging technologies.[321] The Commission assesses that organizational leaders need to: 1) guide careers of subordinates, 2) integrate AI into operational concepts, 3) make resourcing decisions, and 4) add necessary tasks into their organizational goals for the creation of the AI stack. The end result should be savvy leadership that understands the AI ecosystem and how emerging technologies could contribute to large and complex projects, resulting in enhanced lethality, increased readiness, or in cost saving/avoidance; comprehends the risks introduced by rapidly evolving technology and can discriminate between "low hanging fruit", technically ambitious but credible goals, and hype/identify credible technology goals; understands ethical employment of emerging technology; manages competing priorities among future hardware and related software initiatives; applies emerging technologies to current and future national security needs; and better manages the careers of developers and experts.

Recommendation 14 would lay a foundation by teaching junior leaders to understand AI. Building organizational leaders, however, requires engagement with critical technologies throughout their careers. The recommendations below would enable military officers to

[321] NSCAI staff interview with current and former DoD officials (Mar. 24, 2020); NSCAI staff interview with current and former DoD officials (Apr. 23, 2020); NSCAI staff interview with current and former DoD officials (Apr. 26, 2020); NSCAI staff interview with current and former DoD officials (May 1, 2020); NSCAI staff interview with current and former DoD officials (May 22, 2020).

continue building on the foundation in recommendation 14 as they advance and become organizational leaders.

Figure 3.1: AI and Emerging Technology Education Throughout a Military Career



Pre-Commissioning and Initial Training

Recommendation 14:

- Problem definition and curation
- AI Lifecycle
- Data collection and management
- Understanding probabilistic reasoning and data visualization
- Data-informed decision-making

Early and Mid-Career Education

Recommendation 16:

- Integrate emerging technology materials into professional military education
- Emerging technology as defined by USD(R&E)
- Address impact on operations, organizational change, and ethics

Educating Strategic Leaders

Recommendation 17:

- Build on executive education programs at leading universities
- Short courses focused on the latest emerging technology
- Integrate into existing senior leader courses or as stand-alone courses

Time constraints are the main obstacle to becoming emerging technologies conversant. While strategic leaders do not need to become experts in emerging technology, they do need to be aware of the advantages and challenges emerging technologies offer. To avoid this first mover problem, the Congress and Executive Branch senior leaders should intervene, acting as first movers by initiating training and education programs for organizational leaders.[322] This aligns with the *2019 Interim Report* judgement 13, that:

> *National security agencies need to rethink the requirements for an AI-ready workforce. That includes extending familiarity with a range of relevant AI technologies throughout organizations, infusing training on the ethical and responsible development and fielding of AI at every level, and spreading the use of modern software tools.*[323]

It also aligns with judgement 16, that:

> *Expanding AI-focused fellowships and exchange opportunities can give officials and service members access to cutting-edge technology, and bring talent from our top AI companies into federal service.*[324]

Recommendation 1.16: Integrate Emerging Technologies Material into Courses for Officers as part of Service-level Professional Military Education

The DoD should integrate emerging technologies materials into courses for military officers both during officer accession as well in Service-level professional military education. These materials should address AI and other militarily significant emerging technologies, as determined by the military services and the Under Secretary for Defense for Research and Engineering (USD (R&E)). As officers progress in rank, such courses should increasingly build the knowledge base, vocabulary, and skills necessary to intelligently analyze and utilize emerging technologies in the tactical, operational, and strategic levels of warfighting and warfighting support. Integrating emerging technologies material into courses throughout the professional military education cycle of officers' careers will allow officers to better

[322] NSCAI staff interview with government officials (May 5, 2020).
[323] *Interim Report*, NSCAI at 36 (Nov. 2019), https://www.nscai.gov/reports.
[324] Id. at 38.

understand new threats/challenges, better develop operational and organizational concepts, and incorporate technology into operations. Ultimately, a broader understanding of emerging technologies will help officers incorporate a wider range of military applications, tactics, techniques, and procedures into the core functions of Service operations. The DoD should establish a mechanism by which to audit these courses annually, for the first five years of implementation, to ensure that the emerging technologies have been properly identified through USD (R&E) in coordination with the national laboratories federally funded research and development centers (FFRDCs), and university affiliated research centers (UARCs), and that the nomenclature, lexicon, definitions, and course content maintains the accuracy and pace consistent with the evolution across emerging technologies.

Proposed Legislative Branch Action

The Armed Services Committees should use the FY 2022 NDAA to direct the DoD to require emerging technologies courses for officers within one year of FY 2022 NDAA enactment. The Armed Services Committees should also require the DoD to develop a training plan that incrementally builds the necessary skills in its officer corps.

Proposed Executive Branch Action

The DoD should incorporate emerging technology courses for its military officers across all phases of Service-level professional military education and should build on each other as officers progress in rank. The courses should include an introduction to the latest technology, the benefits and challenges of adapting new technologies, and ethical issues surrounding the uses of emerging technologies, including the impact of biases in these technologies.

Recommendation 1.17: Require A Short Course for General and Flag Officers and SES Leadership Focused on Emerging Technologies

The DoD should mandate emerging technology short courses for general and flag officers and SES level organizational leaders. Short courses would focus on educating senior leaders on the latest emerging technology available to help make decisions, improve the decision-making process, streamline organizations, and become emerging tech conversant.[325] This option would be the least time consuming and could appeal to strategic leaders given the time constraints, but the Commission recommends the courses be taken on an iterative basis every two years. It has the smallest barriers to entry, as many senior leaders already attend short, intense courses. These short courses could also be tailored to fit senior leaders' desired outcomes based on organizational needs. The DoD should audit short courses annually at leading universities to ensure nomenclature, definitions, and other information maintains the accuracy and pace consistent with the evolution across emerging technologies.

Proposed Legislative Branch Action

The Armed Services Committee should use the FY 2022 NDAA to require the DoD to establish emerging technologies courses within one year of FY 2022 NDAA enactment. Twenty percent of general or flag officers and SES organizational leaders should be required to pass the course by the end of the first year, with the minimum percentage certified

[325] NSCAI staff interview with SOCOM leaders (Apr. 23, 2020).

increasing by ten percent each year until a minimum of 80 percent of organizational leaders are certified.

Proposed Executive Branch Action

The DoD should require emerging technology short courses for general and flag officers and SES level organizational leaders. The courses should be taught on an iterative, two year basis, should identify the latest, most relevant technologies for senior leaders, analyze how emerging technologies can impact their organization, explain the use of AI by U.S. competition in a global context, and require a level of knowledge about emerging technology to be conversant about the latest technology, trends, and limitations. The course should also take into account how the latest technology can be applied to business or mission outcomes. Senior leaders would be exposed to emerging technology across the interagency; taught how to analyze and evaluate data to determine when to adopt new technologies; how emerging technology can affect organizational change, discover how to leverage technology changes for competitive advantage; and properly evaluate technologies prior to major investment.

Recommendation 1.18: Create Emerging Technology Coded Billets Within the Department of Defense

As the DoD continues to incorporate emerging technologies into its business operations, workforce, and the battlefield, it is crucial that the DoD acquire the talent necessary and maintain the fungible skill sets associated with introducing and fielding emerging technologies within its officer corps. The Commission wants to incentivize and increase the presence of those skills in the uniformed military services. Emerging technologies qualified officers would add value in a number of areas for the services, including: 1) assisting with acquisition of emerging technology, 2) helping integrate technology into field units, 3) developing organizational and operational concepts, and 4) developing training and education plans.

The DoD should create emerging technologies designated billets for officers that require personnel to have achieved an emerging technologies qualification prior to assignment. The joint qualification certification process can serve as a model. The DoD, in accordance with the FY 2007 NDAA,[326] has already designated that certain, critical billets must be filled by Joint Qualified Officers. The Secretary of Defense established different levels of joint qualification, as well as the criteria for qualification at each level.[327]

The Congress and DoD should establish a similar process to designate that certain, critical billets must be filled by emerging technologies qualified officers, and a process for military leaders to become emerging technology qualified. Officers should become emerging technology qualified by serving in emerging technology focused fellowships, emerging technology focused talent exchanges, emerging technology focused positions within government, and educational courses focused on emerging technologies. The Office of the USD (R&E) should define these emerging technologies.

[326] Pub. L. 109-364, John Warner National Defense Authorization Act for Fiscal Year 2007, 109th Cong. (2006)
[327] *DOD Joint Officer Management Program*, DoD Instruction 1300.19 at 14 (Apr. 3, 2018), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/130019p.pdf?ver=2018-04-03-114842-923.

Notably, these billets should not be limited to organizations focused on emerging technology. Instead, roles that significantly interact with or will be significantly impacted by emerging technology should be considered. These include but are not limited to positions that develop military doctrine, operating concepts, positions within Force Structure, Resources, and Assessment directorates and positions within Force Development directorates, and leadership positions at the operational and tactical levels within the military services.

Proposed Legislative Branch Action

The Armed Services committees should use the FY 2022 NDAA to require the DoD to create emerging technology critical billets within the DoD that must be filled by emerging technology certified leaders.

Proposed Executive Branch Action

The DoD should create billets that require officers to become emerging tech certified. These billets should be labeled as emerging tech and would not require a special certification. The process to become emerging tech certified would resemble the joint qualification system, but much less time intensive. Officers could accrue points by participating in fellowships in emerging tech companies, completing courses as described in Recommendation 13, time spent in certain career fields associated with emerging tech (i.e. AI, additive manufacturing, quantum computing, etc.), or time spent in other emerging tech billets.

Issue 7: Creating AI Policy Experts

As mentioned above, policy experts are those who do not lead organizations or develop AI solutions, but need to know enough to inform organizational and national policies. These include some government civilians in organizations like the Office of the Under Secretary of Defense for Policy, and most especially, diplomats in the Department of State. Policy experts who do not understand AI well enough struggle to negotiate effectively with allies and rivals once the subject matter moves beyond shallow topics and begins to require some technical knowledge, thus leaving the United States at a distinct disadvantage during international negotiations, standard setting discussions, and during trade and export policy decision-making processes.[328] As a result, there has been a proliferation of AI-related events where diplomats should represent U.S. interests, but do not have the capacity to do so. This aligns with judgement 13 from the *2019 Interim Report* that:

> *National security agencies need to rethink the requirements for an AI-ready workforce. That includes extending familiarity with a range of relevant AI technologies throughout organizations, infusing training on the ethical and responsible development and fielding of AI at every level, and spreading the use of modern software tools*.[329]

AI can no longer be relegated to a specialized field, understood by a few. NSCAI assessed that training AI policy experts who understand AI beyond generalities will assist with the successful incorporation of AI into the government. AI proficient policy experts can help explain the advantages and disadvantages of AI, help decision makers navigate the ethical

[328] NSCAI staff interview with a former government official (Apr. 24, 2020).
[329] *Interim Report*, NSCAI at 36 (Nov. 2019), https://www.nscai.gov/reports.

and legal implications of its use, and write more precise policies that will ultimately impact the development, implementation, and use of AI.

Recommendation 1.19: Require Short Courses for Policy Personnel with AI-Related Portfolios

Policy experts should attend intensive training provided by either their agency or a contracted group to expose leaders to AI, its capabilities, and policy relevant topics. This could be achieved with short courses on the latest technologies and applications, led by leading universities in the field of AI. Successful models have been run at Harvard University and MIT.[330] It should be noted that while this method requires no organizational changes and requires a relatively small amount of time, it is not immersive, and is likely to create policy experts that are better prepared than they are currently, but still struggle to adequately represent American interests when debating genuine experts from other states. As such, it is a short-term solution.

Proposed Legislative Branch Action

Authorizing committees should mandate that Departments of State, Defense, Commerce, Energy, and Homeland Security, and the ODNI identify policy experts whose portfolios affect or will be affected by AI, then require these personnel to successfully complete short courses covering AI, its capabilities, and policy relevant topics. Authorizing language should mandate the identification of policy experts within 180 days of the passage of legislation, and enrollment in or completion of a short course by 50 percent of the policy experts within two years of the passage of legislation.

Proposed Executive Branch Action

The Departments of State,[331] Defense, Commerce, Energy, and Homeland Security, and ODNI should identify policy experts whose portfolios affect or will be affected by AI, then require these personnel to successfully complete short courses covering AI, its capabilities, and policy relevant topics. These agencies should evaluate current commercial and academic offerings for AI courses, and determine the best fit based on their organization's needs.

[330] MIT's short courses taught by the Sloan School of Business Management and the Computer Science and Artificial Intelligence Laboratory can serve as an example. See *Artificial Intelligence: Implications for Business Strategy (Self-paced Online)*, MIT (last accessed Sept. 26, 2020), https://executive.mit.edu/openenrollment/program/artificial-intelligence-implications-for-business-strategy-self-paced-online/.

[331] This aligns with NSCAI's *Second Quarter Recommendation* for the Department of State to incorporate AI-related technology modules into key Foreign Service Institute training courses, but is intended to apply to other agencies as well. See *Second Quarter Recommendations,* NSCAI at 90-91 (July 2020), https://www.nscai.gov/reports.

Issue 8: Training Acquisition Professionals

The Acquisition Workforce (AWF)[332] often bears the brunt of the blame for the DoD's slow, inflexible acquisition process. Through deeper examination of the issues and interviews with a number of government officials who work within the acquisition system, NSCAI believes these perceptions to be incorrect. While it is clear that the education and training provided to the DoD AWF often lags behind commercial state of the practice, the root cause of this lag can be traced to the DoD's down-stream process that is initiated by legislation or policy changes. The Commission has found that the AWF is constrained by policy, not by an unwillingness or lack of desire to create a more responsive acquisition process.[333] To fully enable adoption of modern digital technologies, including AI and other emerging technologies, the DoD requires an adapted approach to develop and deploy training and education materials to its AWF at the rate of technological change.[334] This aligns with judgement 13 from the *2019 Interim Report* that:

> *National security agencies need to rethink the requirements for an AI-ready workforce. That includes extending familiarity with a range of relevant AI technologies throughout organizations, infusing training on the ethical and responsible development and fielding of AI at every level, and spreading the use of modern software tools.*[335]

Today, the DoD AWF receives its acquisition training and education through the Defense Acquisition University (DAU), which is overseen by the Office of the Under Secretary of Defense for Acquisition and Sustainment (USD (A&S)).[336] As changes to acquisition laws are enacted by Congress or as policies and directives occur at the USD (A&S) level, necessary changes to training and education follow at DAU.[337] This model is not optimized to keep

[332] See *Defense Acquisition Workforce Education, Training, Experience, And Career Development Program*, DoD Instruction 5000.66 (July 27, 2017, Change 2 effective Sept. 13, 2019), https://asc.army.mil/web/wp-content/uploads/2019/11/DoDI-5000.66.pdf.

[333] See also *Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, Defense Innovation Board (Mar. 12, 2019), https://media.defense.gov/2019/Mar/26/2002105909/-1/-1/0/SWAP.REPORT_MAIN.BODY.3.21.19.PDF.

[334] The Defense Innovation Board noted similar findings with regard to software acquisition in particular. See id.

[335] *Interim Report*, NSCAI at 36 (Nov. 2019), https://www.nscai.gov/reports.

[336] See *Defense Acquisition University (DAU)*, DoD Instruction 5000.57 (May 7, 2019), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500057p.pdf?ver=2019-05-07-081600-423 (applying to "OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the 'DoD Components')"); see also *Defense Acquisition Workforce Education, Training, Experience, And Career Development Program*, DoD Instruction 5000.66 (Sept. 13, 2019), https://asc.army.mil/web/wp-content/uploads/2019/11/DoDI-5000.66.pdf (applying to "OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), the Defense Agencies, DoD Field Activities, and all other organizational entities within DoD (referred to collectively in this issuance as the 'DoD Components')").

[337] See *Defense Acquisition University (DAU)*, DoD Instruction 5000.57 (May 7, 2019), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500057p.pdf?ver=2019-05-07-081600-423 (Directing that USD (A&S) "[e]stablishes a program of education and training standards, requirements, and performance learning assets for the civilian and military Defense Acquisition Workforce. The program will promote jointness and interoperability to the greatest extent practical and be designed to provide benefits as broadly as possible to the workforces supporting the A&S mission."); see also *Defense Acquisition Workforce Education, Training, Experience, And Career Development Program*, DoD Instruction 5000.66 (Sept. 13, 2019), https://asc.army.mil/web/wp-content/uploads/2019/11/DoDI-5000.66.pdf ("[e]stablishes policies, assigns

pace with technology trends and maturation of tech-enabled capabilities and, consequently, jeopardizes the military advantage that the United States holds on its global competitors.

To maintain its advantage, the DoD must ensure that its acquisition workforce is positioned to fully leverage the technological capabilities of today, while also proactively planning for delivery of new training and content relevant to technological advancements. Just as the DoD seeks to shorten its sensor-to-shooter timelines to speed decision-making and maintain battlefield dominance, the Department must similarly collapse the time lag in its acquisition system,[338] and drive proactive and continuous evolution across acquisition authorities, policies, and procedures; as well as acquisition training and materials.

As a first step, the Department should develop a classified technology annex to the National Defense Strategy (NDS), as recommended by NSCAI's *Second Quarter Recommendations*.[339] Using this annex as a clear plan for prioritizing and developing disruptive technologies that can help solve the operational challenges identified in the NDS, DoD should then focus on implementing any necessary changes to the acquisition policy or workforce education and training as identified in the annex. By connecting DoD AWF training and education reform directly to the Technology Annex, the Department will adopt a more proactive posture relative to the readiness of its AWF personnel and the system they operate within. Additionally, as NSCAI's *Second Quarter Recommendations* further call for this Technology Annex to be evaluated at least annually, DAU can start to realize a more rapid and scalable approach to evolving its training and education materials.

The following recommendations are designed to increase the efficacy of acquisition education and training programs in the near- and medium-term relative to emerging technologies that our national security organizations have already cited as critical.[340]

Recommendation 1.20: Require Emerging Technology Training for Specific Acquisition Functional Areas

Acquisition workforce leaders should identify training specific to the acquisition workforce functional areas deemed essential to make informed emerging technology purchases.[341] This option would require no modification of the current acquisition workforce; rather, it would require changes to existing acquisition training curriculum in order to focus government acquisition workforce civilians on the unique challenges that emerging technologies pose to

responsibilities, and provides procedures for the conduct of the Defense Acquisition Workforce (AWF) Education, Training, Experience, and Career Development Program").

[338] Used here to include the DoD's acquisition authorities, policies, and procedures in addition to acquisition workforce training content and curricula.

[339] *Second Quarter Recommendations*, NSCAI at 24-26 (July 2020), https://www.nscai.gov/reports.

[340] *Summary of the 2018 National Defense Strategy of the United States of America*, U.S. Department of Defense at 7 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[341] Section 862 of the FY 2020 NDAA similarly directs that "[t]he Secretary of Defense, acting through the Under Secretary of Defense for Acquisition and Sustainment and in consultation with the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Personnel and Readiness, and the Chief Information Officer of the Department of Defense, establish software development and software acquisition training and management programs for all software acquisition professionals, software developers, and other appropriate individuals (as determined by the Secretary of Defense), to earn a certification in software development and software acquisition." See Pub. Law 116-92, sec. 862, National Defense Authorization Act for Fiscal Year 2020, 116th Cong. (2019). However, this and the DIB SWAP Implementation Working Group are focused specifically on software acquisition vice emerging technology more broadly.

their specific acquisition functional areas. This would afford leaders the most flexibility to focus training on specific acquisition functional areas to better understand how to best incorporate emerging technologies into those acquisition functional areas and associated processes. This would also avoid blanket, one-size-fits-all training for the entire acquisition workforce that might be tangentially related. The end result would be a more relevant set of training topics that apply to assigned duty functional areas, could integrate design thinking and leaner acquisition methodologies.

Proposed Legislative Branch Action

The Armed Services Committees should use the FY 2022 NDAA to require the DAU to annually assess the AWF's need for additional emerging technology education and to design and offer functional area specific courses to meet those needs.

Proposed Executive Branch Action

The DAU, in partnership with USD (R&E), should annually assess the AWF's emerging technology education needs. As necessary, DAU should design and offer courses addressing new AWF needs. These courses should be tailored to specific acquisition functional areas.

Recommendation 1.21: Support DAU Pilot Programs Attempting to Use AI to Tailor Pedagogy and Content to Individuals

DAU has begun pilot programs aiming to use AI to both curate existing DoD AWF curriculum content as well as to tailor the delivery of that content to individual users. If successful, this approach could not only allow for more rapid tailoring and updating of content, but allow for individual students to receive DoD AWF training that best aligns to their individual positions, roles, and functions within the DoD AWF as well as to the specific level of program that they individually support. This approach could also allow for a better understanding of the modality of training delivery to tailor content delivery differently for each student. This is a longer-term project, but it could provide for the most tailored acquisition workforce training to date, delivered at a quicker pace than normal training, and delivered in the best modality for the individual acquisition workforce employee. By utilizing AI-selected and tailored training sessions, acquisition training course developers could provide the most up-to-date materials and ensure that industry best practices, government acquisition lessons learned, and other dynamically changing materials could be easily and rapidly incorporated to keep training materials relevant in a much more rapid timescale than can be done today.

Proposed Executive Branch Action

The DoD should ensure that USD (A&S) properly resources DAU for these pilots and provide routine reports on their successes or barriers to success. Additionally, the DoD should evaluate current commercial and academic offerings for AI-enabled curriculum development and management that might be suitable for government use, as the NSCAI is aware of similar projects that have had success in academia that could potentially translate to success at DAU.

Part II: Recommendations to Improve STEM Education

One of the greatest investments that the United States Government can make to secure its future is to invest in education for all of its people. The NSCAI has, since its outset, focused on the gaps in talent and workforce that our nation needs in order to remain a global leader in artificial intelligence. As the Commission's *2019 Interim Repor*t states, "People are still essential. Talent remains the most important driver of progress in all facets of AI. The United States must prioritize cultivating homegrown talent by making long-term investments in STEM education."[342]

AI is becoming ubiquitous, but the United States continues to have a lack of available AI talent. As a result, our nation faces a host of serious national security challenges that are made worse as the demand for such talent creates inflated salaries, as AI talent then leaves academia in pursuit of those salaries, and as the gap between the workforce that nation needs and the talent available continues to widen.[343] The nation needs to increase efforts to provide a strong STEM education to all Americans in order to create a strong economy and increase the available talent, thereby increasing our ability to compete globally and improve national security. And, NSCAI continues to focus on improving AI literacy, and the underlying STEM foundation that AI literacy requires, as it is part of our Congressionally-mandated charter.

In this age of great power competition, our nation's economy is an important measure of our national strength. The American economy relies on an innovation economy to generate jobs and income.[344] In particular, science and engineering employment in the United States—such as software developers, computer system analysts, chemists, mathematicians, economists—has grown more rapidly than the workforce overall and now represents 5 percent (about 7 million) of all U.S. jobs.[345] The median salary for those jobs (across workers at all education levels) was $85,390, more than double the median for all U.S. workers.[346] Jobs in artificial intelligence have experienced exponential growth. Since 2010, AI-related jobs have tripled annually and accounted for almost 3 million jobs in the United States by 2019.[347] By 2030, it has been estimated that AI-related jobs will account for $13 trillion of global GDP.[348]

[342] *Interim Report,* NSCAI at 16 (Nov. 2019), https://www.nscai.gov/reports.

[343] Stuart Zweben & Betsy Bizot, *2019 Taulbee Survey: Total Undergrad CS Enrollment Rises Again, but with Fewer New Majors; Doctoral Degree Production Recovers From Last Year's Dip*, Computing Research Association at 11 (May 2020), https://cra.org/wp-content/uploads/2020/05/2019-Taulbee-Survey.pdf.

[344] For this paper, the Commission uses Joseph Schumpeter's model of "innovation economy" that credits evolving institutions, entrepreneurship, and technological change as the centerpiece for economic growth. See Joseph Schumpeter, *Capitalism, Socialism, and Democracy* (1942).

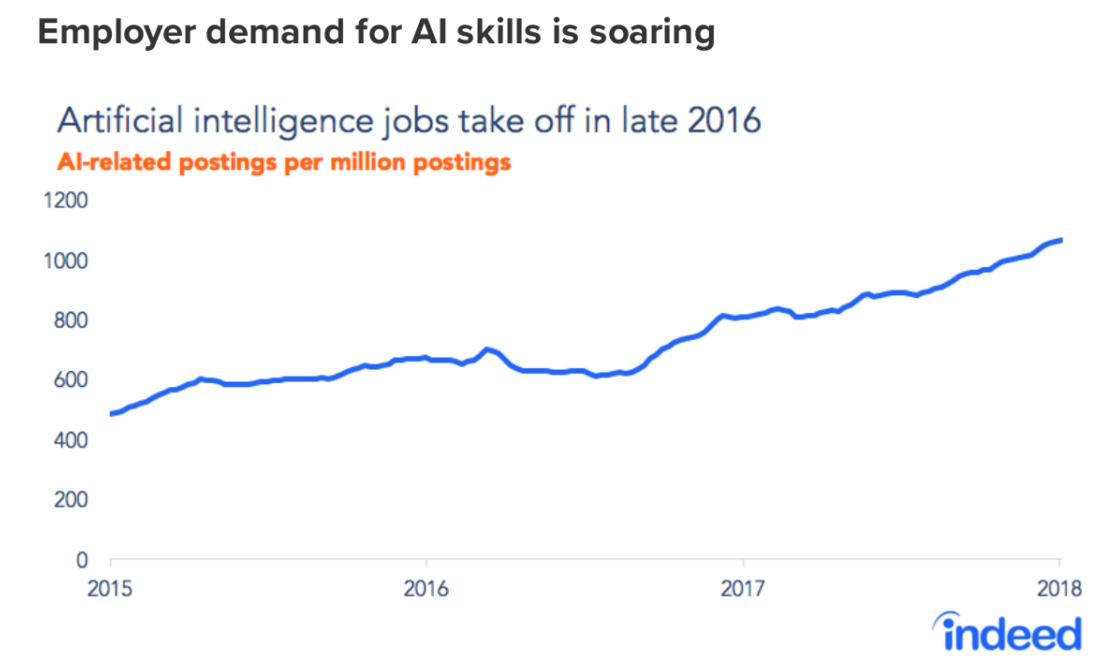
[345] *2020 National Science Board Science and Engineering Indicators: The State of U.S. Science and Engineering*, National Science Board at 6 (Jan. 2020), https://drive.google.com/file/d/1MwkKm9f2r13o9G6tWEdhPcsNxxoms9Ou/view?usp=sharing.

[346] Id. The median salary of the average U.S. worker is $37,690. Id.

[347] The calculation was determined by jobs captured by Burning Glass, a company that specializes in job market trends and analysis. See Autumn Toney & Melissa Flagg, *U.S. Demand for AI-Related Jobs,* Center for Security and Emerging Technology at 3 (Aug. 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-US-Demand-for-AI-Related-Talent.pdf.

[348] Id. at 2 (citing a 2018 McKinsey Global Institute report).

Figure 3.2: Trends in Employer Demand for AI Skills



Source: indeed[349]

As AI becomes ubiquitous across sectors, demand for AI talent will grow further. There is a need to create pipelines for different levels of skills—from PhDs that will unlock new frontiers of the technology to someone employing AI into their business operation, to average citizens who need the knowledge to frame interaction with the technology in daily life. This includes roles in national security where the United States needs more citizens with the requisite skills and backgrounds to fill the variety of roles the Commission outlined in its *2019 Interim Report*.

The underlying engine to enable AI jobs is our nation's education system and the talent that it produces. This is particularly the case for STEM education, as without a proper STEM foundation, students cannot succeed in becoming the AI practitioners that this country needs. In this regard, a number of indicators show that the United States is lagging its primary competitors, including China.[350] These include, but are not limited to the Programme for International Student Assessment (PISA) and the Trends in International Mathematics and Science Study (TIMSS).

The PISA is an international assessment that measures reading ability, math and science literacy, and other skills among 15-year-old students. In the most recent PISA in 2015, "[t]he United States ranked thirty-eighth out of seventy-one countries in math and twenty-fourth in

[349] Daniel Cublertson, *Demand for AI Talent on the Rise*, Indeed: Hiring Lab (Mar. 1, 2018), https://www.hiringlab.org/2018/03/01/demand-ai-talent-rise/#:~:text=Employer%20demand%20for%20AI%20skills%20is%20soaring&text=Demand%20for%20workers%20with%20AI%20talent%20has%20more%20than%20doubled,over%20the%20past%20year%2C%20too.
[350] As of 2016, in STEM fields alone, China graduated 4.7 million students; the United States graduated 568,000. See Arthur Herman, *America's High-Tech Stem Crisis*, Hudson Institute (Sept. 10, 2018), https://www.hudson.org/research/14547-america-s-high-tech-stem-crisis.

science. Among the thirty-five members of the Organisation for Economic Co-operation and Development (the PISA's principal sponsor), the United States comes in fifth from the bottom in math and nineteenth in science."[351]

Similarly, the TIMSS is an international assessment of students in the fourth and eighth grades that has taken place every four years since 1995. According to one expert:

> *Again, in the most recent [TIMSS] test from 2015, ten countries (out of forty-eight total) had higher average fourth-grade math scores than the United States, while seven countries had higher average science scores. In the eighth-grade tests, seven out of 37 countries had statistically higher average math scores than the United States, and seven had higher science scores. In the fourth-grade math category, Japan, South Korea, Taiwan, England, and Norway all scored higher—as did China and Russia.*[352]

One might look at these education performance assessments and assume that the underlying issue here is a lack of funding by the United States on education. On the contrary, U.S. spending per student has continually risen and places the United States as a top spender on education on a per student basis. In 2016, the United States spent $13,600 per student, which was the fifth highest total per student in the world, and $31,600 per student at the post-secondary level, which was first in the world.[353] The distribution of spending per student is misleading if examined only at a national level. Individual state spending varies widely, with some states spending as little as roughly $7,000 per student and others spending as much as $22,000 per student.[354]

Spending per student is likely a mediocre predictor of student performance on test taking, as evidenced by only three of the top ten states of per student spending finishing in the top third of fourth grade math testing.[355] Unfortunately, a far better predictor of success is individual student's race and/or economic status. In 2019, when compared to their White student counterparts, Black students scored an average of 25 points lower and Hispanic students scored an average of 18 points lower.[356] Similarly, students who were eligible for the National Lunch School Program scored 24 points lower than those students who were ineligible.[357]

Some states have already taken the initiative to increase STEM education and their efforts have resulted in progress in STEM education and their own economies. Through a mixture of federal, states, and local investments, Oregon leveraged over $7 million for STEM Hubs across the state.[358] In 2017, Oregon added 50,600 jobs, seeing the fifth fastest job growth in

[351] Arthur Herman, *America's STEM Crisis Threatens Our National Security*, American Affairs (Spring 2019), https://americanaffairsjournal.org/2019/02/americas-stem-crisis-threatens-our-national-security/.

[352] Id.

[353] *Education Expenditures by Country*, National Center for Education Statistics (May 2020), https://nces.ed.gov/programs/coe/indicator_cmd.asp.

[354] *Education Spending Per Student by State*, Governing the Future of States and Localities (last accessed Sept. 23, 2020), https://www.governing.com/gov-data/education-data/state-education-spending-per-pupil-data.html.

[355] Id.; *The Nation's Report Card*, National Center for Educational Statistics (2019), https://nces.ed.gov/nationsreportcard/subject/publications/stt2019/pdf/2020013NP4.pdf.

[356] *The Nation's Report Card*, National Center for Educational Statistics (2019), https://nces.ed.gov/nationsreportcard/subject/publications/stt2019/pdf/2020013NP4.pdf.

[357] Id.

[358] *Advancing STEM Education in Oregon: STEM Investment Council, Regional STEM Hubs, and STEM Innovation Grants*, Higher Education Coordinating Commission at 15 (Feb. 2019),

the nation. This growth—and future projected job growth—is largely attributed to demand in STEM fields.[359] West Virginia has made similar investments in its STEM education and has estimated that 205 STEM jobs are created each year for an increase of over half a million dollars in state revenues each year.[360]

Investments in STEM education will have a massive positive impact on the ability of the United States to compete globally. By increasing the quality of education for all Americans, the entire national pool of digital talent will increase, greater segments of the population will have access to higher paying jobs, and a greater number of Americans will contribute to the economic security of the United States.

For all of the opportunities that STEM jobs can bring to the United States, if systemic challenges to our educational system are not addressed, those career fields will stagnate and stymie economic growth. The Federal Government must take an active role in incentivizing STEM education for all Americans with programs that help the states to provide more equitable access to all students and help to prepare the developing workforce to realize the full potential of future economic opportunities.[361] The National Science and Technology Council found that:

> *Basic STEM concepts are best learned at an early age—in elementary and secondary school—because they are the essential prerequisites to career technical training, to advanced college-level and graduate study, and to increasing one's technical skills in the workplace. Increasing the overall digital literacy of Americans and enhancing the STEM workforce will necessarily involve the entire U.S. STEM enterprise.*[362]

Properly targeted federal funding across the continuum of America's students—from the beginning of children's education through their teenage years as they progress through the U.S. education system—can improve the overall quality, diversity, and quantity of STEM talent.

The current model of STEM education in America will not meet the challenges of tomorrow. While the Commission is heartened by the recent developments to provide more

https://www.oregon.gov/highered/research/Documents/Reports/STEM-Investment-Council-%20Legislative-Report-February-2019-FINAL.pdf.

[359] Id. at 7. "In fact, the Oregon Employment Department projects more than 430,000 job openings in STEM fields in Oregon between 2017 and 2027 – a growth rate of 15 percent, or 3 percent higher than the projected growth rate for all jobs in Oregon during the same 10-year period. Moreover, roughly 93 percent of the projected job openings in STEM fields are in high wage occupations and about 90 percent are in high demand occupations. To fill these jobs and continue growth, Oregon's employers need – now and in the future – a STEM-literate workforce." Id.

[360] *Our Impact*, WVUteach (last accessed Sept. 23, 2020), https://wvuteach.wvu.edu/about/roi.

[361] Studies conducted by the OECD found that "[i]f the United States were to ensure that all of its students had basic skills, the economic gains could reach over $27 trillion in additional income for the economy over the working life of these students. So even high-income OECD countries would gain significantly if all of their students left school with at least basic knowledge and skills. For this group of countries, the average future GDP would be 3.5% higher than it would be without this improvement. That is close to what these countries now spend on school education. In other words, the economic gains that would accrue solely from eliminating extreme underperformance in high-income OECD countries by 2030 would more than pay for the primary and secondary education of all students." Andreas Schleicher, *World Class: How to Build a 21st-Century School System*, OECD at 143 (2018), https://www.oecd.org/education/world-class-9789264300002-en.htm.

[362] *Charting a Course for Success: America's Strategy for STEM Education*, National Science and Technology Council at v, (Dec. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/12/STEM-Education-Strategic-Plan-2018.pdf.

equitable access to broadband internet, the devices and services needed to take advantage of it, and investments in low-performing school districts, all of which are vital to improving STEM education and providing better pathways to develop AI practitioners, more needs to be done if the United States is to achieve a competitive edge in AI and other related advanced technologies.

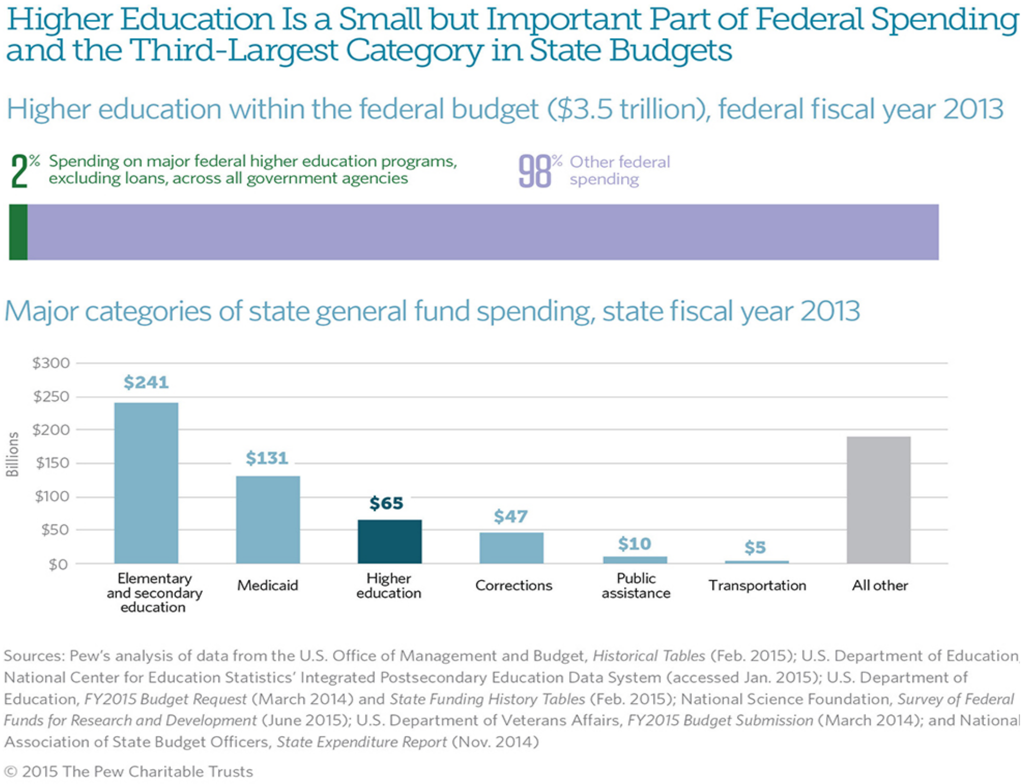
This set of recommendations is designed to address STEM education, specifically those areas the Commission believes will boost American innovation in AI. The Commission's recommendations address needs for undergraduate and postgraduate education, and reskilling/upskilling of workers once they are in the workforce.[363] The Commission acknowledges that providing equitable access to quality STEM education to all Americans will require recommendations for change that exceed the mandate of this Commission. However, there is no way to improve the level of AI literacy in the United States without broader initiatives like the ones outlined below.

Issue 1: Strengthening Universities as Talent Pipelines

STEM education at the university level in America is among the least prioritized in federal budgets, but federal funding in this area is a major source of education revenue at the state level. According to Pew research, federal spending takes up 2 percent of the federal budget, but is the third highest category of spending that states rely on for higher education (see below).

[363] STEM education in America, particularly the university system, relies on international talent in its undergraduate and graduate degree programs, as well as faculty. NSCAI is planning to address the issue of attracting and retaining international talent separately.

Figure 3.5: Federal and State Funding of Higher Education


Higher Education Is a Small but Important Part of Federal Spending and the Third-Largest Category in State Budgets

Sources: Pew's analysis of data from the U.S. Office of Management and Budget, *Historical Tables* (Feb. 2015); U.S. Department of Education, National Center for Education Statistics' Integrated Postsecondary Education Data System (accessed Jan. 2015); U.S. Department of Education, *FY2015 Budget Request* (March 2014) and *State Funding History Tables* (Feb. 2015); National Science Foundation, *Survey of Federal Funds for Research and Development* (June 2015); U.S. Department of Veterans Affairs, *FY2015 Budget Submission* (March 2014); and National Association of State Budget Officers, *State Expenditure Report* (Nov. 2014)

© 2015 The Pew Charitable Trusts

Source: The Pew Charitable Trusts[364]

Universities across America have been forced to become more reliant on state budgets, which has also been an unreliable source of funding for STEM education. As states' budgets tighten due to the COVID-19 pandemic, universities will be forced to find different revenue streams and might cut vital programs.[365] Numerous interviews with leaders in STEM education have stated that improving STEM education in the United States will require a significant investment by the Federal Government.[366]

Recommendation 2.1: National Defense Education Act II

The National Defense Education Act (NDEA) of 1958 is widely regarded as the most successful piece of education legislation in the United States.[367] The NDEA greatly increased the number of Americans with a college degree, expanded the number of math and science teachers to meet the demand of the K-12 educators after the post-war baby boom, and was

[364] Ingrid Schroeder & Anne Stauffer, *Federal and State Funding of Higher Education*, Pew Charitable Trusts at 2 (June 2015), https://www.pewtrusts.org/~/media/assets/2015/06/federal_state_funding_higher_education_final.pdf.

[365] Melissa Korn, *Public Colleges Lose State Funding, Effective Immediately*, Wall Street Journal (Apr. 23, 2020), https://www.wsj.com/articles/public-universities-see-state-funding-disappear-effective-immediately-11587653753.

[366] NSCAI staff interview (June 26, 2020); NSCAI staff interview (July 1, 2020); NSCAI staff interview (July 6, 2020); NSCAI staff interview (July 10, 2020).

[367] Pamela Flattau, *The National Defense Education Act of 1958: Selected Outcomes*, Institute for Defense Analysis Science & Technology Policy Institute (Mar. 2006), https://www.ida.org/-/media/feature/publications/t/th/the-national-defense-education-act-of-1958-selected-outcomes/d-3306.ashx.

focused on defense-centric fields, particularly a deficiency in mathematicians.[368] The impacts of federal spending on university level education today are echoes of the investments made in the late 1950s by the Eisenhower administration.

Just as the United States once used the NDEA to produce a generation of science talent, it should now aggressively invest in America's education system to maintain world leadership in STEM, particularly in AI and emerging technology by passing an NDEA II. As evidenced above, the current pace of STEM degrees granted in the United States university system will not meet the demand of jobs.[369] The COVID-19 pandemic threatens the emergence of new STEM graduates in fields where they may be well positioned to develop technological responses to future crises—a problem that will worsen if steps are not taken to mitigate these effects. Ambitious investments along the lines proposed by other recent task forces are warranted.

The proposed National Defense Education Act II is based off of an independent task force sponsored by the Council on Foreign Relations (CFR) proposed funding 25,000 STEM undergraduate scholarships, 5,000 STEM graduate fellowships, and NSCAI is recommending an additional 500 postdoctoral positions.[370] The Commission agrees with this proposal and recommends that Congress should authorize the National Science Foundation to spend $8.05 billion to grant 25,000 STEM undergraduate scholarships and 5,000 STEM fellowships over a five year period. Congress should also designate 25 percent of the total number of scholarships and fellowships for underrepresented groups in STEM fields. Congress should also designate 25 percent of those scholarships for AI or AI-enabling fields. Each scholarship and fellowship should cover full tuition and a stipend of $25,000.[371]

Given the acute lack of STEM teachers and tenure-track faculty, some of these postdoctoral awards should be dedicated to those who are committed to teaching. There is currently a nation-wide shortage of qualified computer science professors in the United States. Bachelor's degrees in computer science increased by 74 percent between 2009 and 2015 and PhD programs experienced a 300 percent increase over the same period.[372] Of the 2018-2019 class of PhD graduates, only 31.5 percent went into an academic position after graduation.[373] The hiring situation at some universities is so challenging that 18 percent of tenure-track faculty openings failed to hire any faculty.[374] Congress should also authorize the National Science Foundation to spend $175 million to grant 1,000 two-year postdoctoral

[368] Id.

[369] *Engage to Excel: Producing One Million Additional College Graduates with Degrees in Science, Technology, Engineering, and Math*, President's Council of Advisors on Science and Technology at 1 (Feb. 2012), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-engage-to-excel-final_2-25-12.pdf. The report found that the percentage of STEM occupations will rise from 5.0 percent to 5.3 percent of total jobs in America, which would necessitate an increase of 1 million degrees in STEM programs. Id. at 2.

[370] James Manyika & William H. McRaven, *Innovation and National Security: Keeping Our Edge*, Council on Foreign Relations (Sept. 2019), https://www.cfr.org/report/keeping-our-edge/recommendations/.

[371] The recommended appropriation assumes that 25,000 students will receive four year scholarships and 5,000 students will receive three year fellowships at a cost of $70,000 per student per year.

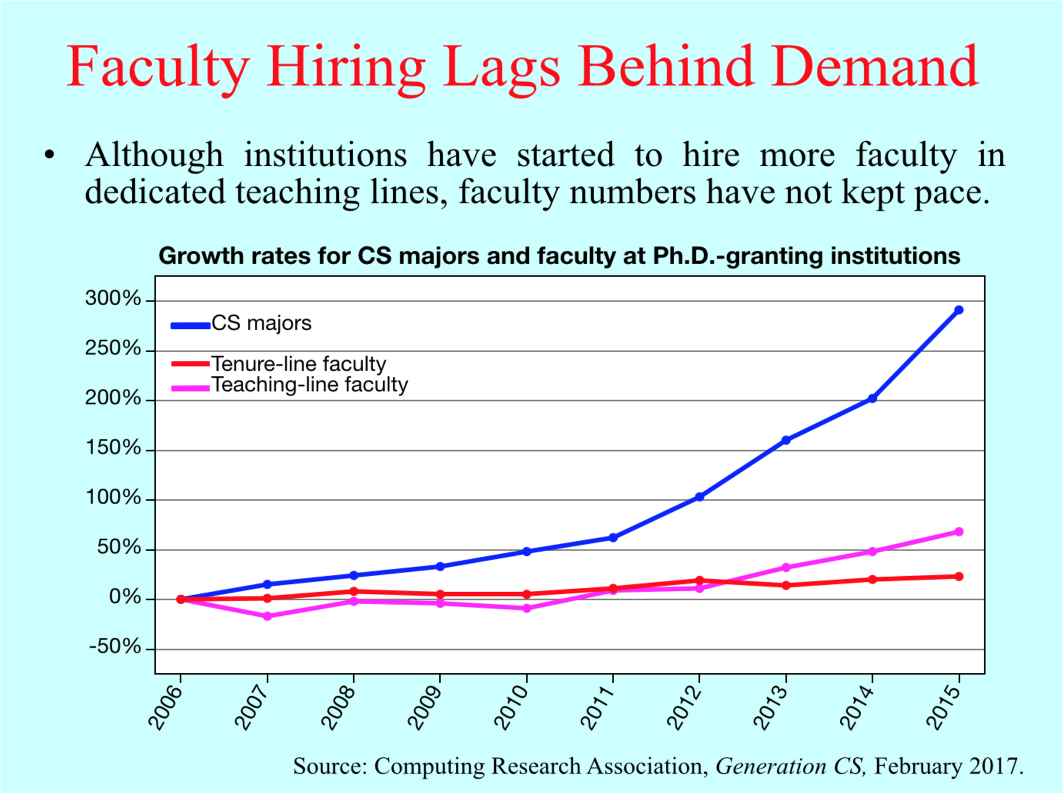
[372] Colleen Flaherty, *System Crash*, Inside Higher Education (May 9, 2018), https://www.insidehighered.com/news/2018/05/09/no-clear-solution-nationwide-shortage-computer-science-professors.

[373] Stuart Zweben & Betsy Bizot, *2019 Taulbee Survey: Total Undergrad CS Enrollment Rises Again, but with Fewer New Majors; Doctoral Degree Production Recovers From Last Year's Dip*, Computing Research Association at 11 (May 2020), https://cra.org/wp-content/uploads/2020/05/2019-Taulbee-Survey.pdf.

[374] Craig Wills, *Outcomes of Advertised Computer Science Faculty Searches for 2017*, Computing Research Association (Nov. 2017), https://cra.org/crn/2017/11/outcomes-advertised-computer-science-faculty-searches-2017/.

fellowships for PhD graduates who intend to remain in academia.[375]

Figure 3.6: Trends in Computer Science Faculty Hiring



Faculty Hiring Lags Behind Demand

- Although institutions have started to hire more faculty in dedicated teaching lines, faculty numbers have not kept pace.

Source: Computing Research Association, *Generation CS,* February 2017.

Source: Computing Research Association[376]

For the purposes of AI, this investment into computer science would have a number of benefits for universities and students. This investment would support more U.S. computer science students staying in academia as opposed to going to the private sector, which would help with the drain of talent from academia. The legislation could also be written to allow flexibility for students to enter the private sector, but return to continue their studies.

Proposed Legislative Branch Action

The Senate Committee on Health, Education, Labor and Pensions and House Committee on Education and Labor should support the National Defense Education Act II. Appropriators should set aside $8.05 billion for NDEA II to fund 25,000 students to receive four year scholarships and a total of 5,000 students that would additionally receive three year fellowships—each at a cost of $70,000 per student per year. Congress should also authorize

[375] Historically, similar postdoctoral fellowships have cost roughly $175,000 per two-year fellowship to cover salaries, benefits, mentorship experiences, and ancillary costs. See e.g., *Computer and Information Science and Engineering (CISE) Research Initiation Initiative (CRII)*, National Science Foundation (last accessed Sept. 30, 2020), https://www.nsf.gov/pubs/2020/nsf20593/nsf20593.htm.

[376] Colleen Flaherty, *System Crash*, Inside Higher Ed (May 9, 2018), https://www.insidehighered.com/news/2018/05/09/no-clear-solution-nationwide-shortage-computer-science-professors.

the NSF to spend $175 million to grant 1,000 two-year postdoctoral fellowships for PhD graduates who intend to remain in academia.

Recommendation 2.2: Mid-Career Faculty Fellowships

NSCAI's *2019 Interim Report* noted the trend of AI experts leaving academia for industry as a problem for cutting edge R&D research.[377] This trend is also important to note for faculty who teach computer science and other STEM related classes. On average, research universities must replace half of their STEM faculty over a 10-year period.[378] Difficulties retaining quality faculty to teach necessary STEM skills are problematic and could cause issues as the number of students in STEM fields rise. As noted above, the number of students pursuing computer science degrees has increased significantly in recent history. If left unaddressed, this could inhibit the number of computer science degrees and hurt the overall quality of students' education. Maintaining this link of mid-career experts is crucial in training the next generation of AI and STEM experts.[379]

A remedy for the keeping quality STEM teaching talent in universities is a mid-career fellowship for recently tenured faculty. Creating a new funding stream for STEM faculty will encourage more research and teaching at a high level in academia. In a competitive market for STEM talent, it is imperative to incentivize seasoned faculty to remain in academia and provide opportunities to do exciting work that they might only find in the private sector.

The NSF currently has several mid-career fellowships that include biological sciences. This program provides an opportunity for a mid-career researcher at the associate professor rank to enable a new synthesis of their ongoing research. By NSF's definition, "[t]his track aims to provide mid-career scientists with new capabilities to enhance their productivity, improve their retention as scientists, and ensure a diverse scientific workforce that remains engaged in active research (including more women and minorities at high academic ranks)."[380] NSF could also recognize and support outstanding faculty in AI or AI applied with a similar mid-career award.

Proposed Legislative Branch Action

The Senate Committee on Health, Education, Labor and Pensions and House Committee on Education and Labor should support the mid-career fellowship award for AI. Appropriators should set aside $15 million for the fellowship.

[377]See *Interim Report*, NSCAI at 25 (Nov. 2019), https://www.nscai.gov/reports; see also Tony Peng & Michael Sarazen, *Are Commercial Labs Stealing Academia's AI's Thunder?*,
Synced Review (July 10, 2019), https://medium.com/syncedreview/are-commercial-labs-stealing-Academias-ai-thunder-dd51cf4bd8d6. One study identified 221 AI faculty from North American universities who departed academia for an industry job from 2004-2018. In a sign of the acceleration of the trend, 40 of these moves occurred in 2018 alone. See Michael Gofman & Zhao Jin, *Artificial Intelligence, Human Capital, and Innovation*, University of Rochester at 3, 39 (Aug. 20, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3449440.

[378] Deborah Kaminski & Cheryl Geisler, *Survival Analysis of Faculty Retention in Science and Engineering by Gender*, Science at 864, (Feb. 17, 2012), http://sitc-portal.isoveradev.com/sites/default/files/post-files/864.full_.pdf. Since the issue of retention for both fields are glaring, the Commission will combine "AI" and "STEM" in this recommendation for clarity.

[379] *First Quarter Recommendations*, NSCAI at 27 (Nov. 2019), https://www.nscai.gov/reports.

[380] *Opportunities for Promoting Understanding through Synthesis (OPUS)*, National Science Foundation (Aug. 5, 2019), https://www.nsf.gov/pubs/2018/nsf18582/nsf18582.htm.

Recommendation 2.3: Support Creation of Pilot Program for Artificial Intelligence Technology and Education Improvements for Community Colleges

Strengthening the ability of U.S. universities to train and equip the next generation workforce for a future in which AI and advanced technologies are ubiquitous requires democratization of access to AI degree and certificate granting programs in post-secondary institutions. In addition to finding faculty to teach computer science and AI classes, a roadblock to beginning those programs is curriculum availability. Much like the curriculum for K-12 educators, this would be an opportunity to accelerate institutions' ability to teach computer science and AI and improve standards for those universities who already teach those subjects.

Congress should fund a program within the Department of Education's Fund for the Improvement of Postsecondary Education (FIPSE) to provide grants to universities to create undergraduate and graduate degree programs for AI and computer science, as well as minor and certificate programs to educate undergraduate and graduate students in other fields on the fundamentals of advanced computing and AI.

FIPSE currently funds a Pilot Program for Cybersecurity Education Technological Upgrades for Community Colleges (PPCETUCC), which could serve as a template for similar AI programs at community colleges. The PPCETUCC program is a "designed program to support technology upgrades for community colleges for the purpose of supporting cybersecurity programs. The efforts of the nation's community colleges to expand cybersecurity education in lower-income student populations are commendable and important, but often those schools lack the resources to maintain state of the art programs."[381] Under this pilot program, participating community colleges receive funding to "purchase, install, and populate a virtual lab environment [...], along with the required server infrastructure, on-site support and miscellaneous hardware."[382] This program enables community colleges to build state-of-the-art facilities and cybersecurity spaces that gives students access to the latest technology.

Such a program could support up-front costs of universities in creating these degree and certificate programs, which are in-demand across the country.[383] Furthermore, it could help create a community of practice across the university landscape to accelerate innovations and create pathways for more articulation agreements between community colleges, technical colleges, federal agencies and degree granting universities.

In order to address the growing need for a wide range of AI proficient workers, the Federal Government should invest in a new pilot program for AI upgrades for community colleges. The new pilot program, the Artificial Intelligence Technology and Education Improvement Program (AITEIP) program, should mirror the technical and infrastructure requirements for

[381] Pilot Program for Cybersecurity Education Technological Upgrades for Community Colleges, U.S. Department of Education (last accessed Sept. 23, 2020), https://www2.ed.gov/programs/ppcetucc/index.html.
[382] Project Abstracts for the Pilot Program for Cybersecurity Education Technological Upgrades for Community Colleges, U.S. Department of Education at 1 (2018), https://www2.ed.gov/programs/ppcetucc/awards.html.
[383] In NSCAI interviews, university representatives from schools with AI programs communicated that they can't keep up with the level of demand for CS and AI courses at the undergraduate level.

PPCETUCC, but NSCAI recommends that AITEIP grant proposals should include funding for the creation of AI curricula and ways to promote private sector cooperation.

Proposed Legislative Branch Action

Congress should establish an AITEIP pilot program for community colleges. Appropriators should set aside $30 million for the AITEIP pilot program.[384]

Recommendation 2.4: Creation of AI-Specific Government Internships

Internships are a stepping stone to full-time jobs, especially within the Federal Government. Paid internships turn into official job offers about 65 percent of the time.[385] Currently, there are few to no government internships that specifically focus on artificial intelligence. DoD has the DoD STEM program, which is a combination of fellowships, scholarships, and internships for STEM students to increase the government's talent pool to these individuals.[386] There are a multitude of Computer Science and Cybersecurity Internships within the Federal Government, however none of these emphasize the importance of AI research and its growth. Similarly, Energy has the Artificial Intelligence and Technology Office, which covers a variety of AI-specific topics, and NIST conducts research on AI technology and standards.[387] None of these programs and agencies give students opportunities to work with AI and conduct AI R&D. The vast majority of AI internships lie within the private sector, meaning the government is losing potential hires in AI and STEM education.

NSCAI's *First Quarter Recommendations* included the expansion of the Pathways Internship Program.[388] While this is a similar recommendation, there are a multitude of difficulties in expanding and changing an existing program, such as ensuring each agency has the desire and capability to change. However, creating an AI-specific internship would allow agencies to create a whole new program as they see fit rather than abiding by specific rules and regulations of a previous program. This is not to say that AI-specific internships will not become potential Pathways internships in the future. As more schools develop AI majors and degrees, there is a need for these students to experience and work in their fields prior to graduation. In order to increase AI knowledge and capabilities within the government, the Departments of Defense and Energy, as well as the National Institute of Standards and Technology, should create paid AI-specific internship positions that focus on AI R&D, AI application, and other related AI topics.

[384] This figure is based off of grant proposals listed on PPCETUCC's website. A comparable pilot focused on artificial intelligence at a cost of up to $200,000 per community college would equate to a minimum of 150 supported sites, taking into account an expected increased cost of the required AI stacks, including compute, that may need to be built at each site. *Awards - Pilot Program for Cybersecurity Education Technological Upgrades for Community Colleges*, U.S. Department of Education (last accessed Sept. 23, 2020), https://www2.ed.gov/programs/ppcetucc/awards.html.

[385] Benjamin Steele, *Interns More Likely to be Hired as Full-Time Employees*, The Daily Universe (Feb. 22, 2017), https://universe.byu.edu/2017/02/22/interns-more-likely-to-be-hired-as-full-time-employees/ (citing a study by the National Association of Colleges and Employers).

[386] *DoD STEM: STEM Education Programs*, U.S. Department of Defense (last accessed Sept. 23, 2020), https://dodstem.us/.

[387] *Artificial Intelligence and Technology Office*, U.S. Department of Energy (last accessed Sept. 23, 2020), https://www.energy.gov/ai/artificial-intelligence-technology-office.

[388] *First Quarter Recommendations*, NSCAI at 38-39 (Mar. 2020), https://www.nscai.gov/reports.

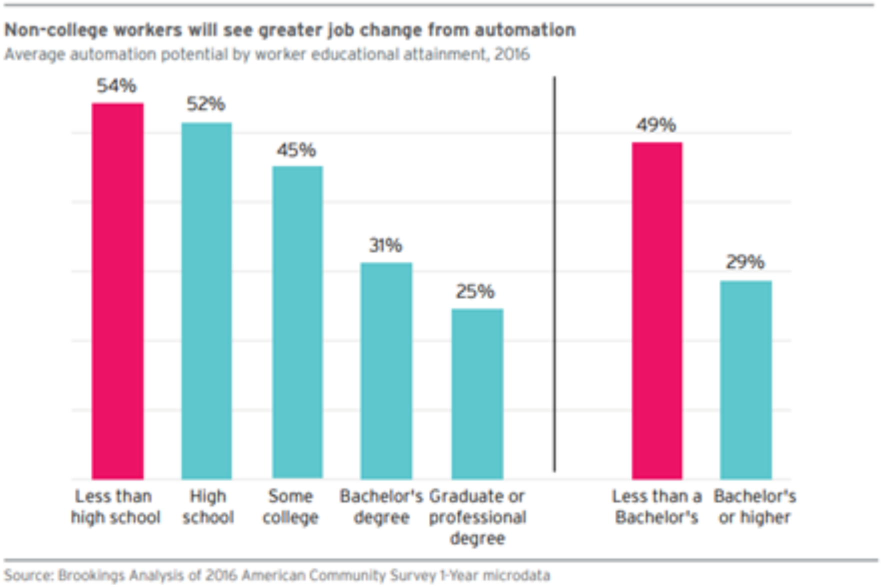
Proposed Legislative Branch Action

Congress should support the creation of an AI-specific internship program for utilization across the Federal Government. Appropriators should set aside $2 million for the program for the creation of 340 internships.[389]

Issue 2: Reskilling the Workforce

AI and automation have had a profound impact on the American economy. Almost all occupations will find some level of exposure to AI in the coming decades and some even face replacement by automation.[390] A study by Brookings Institution found that the lower an individual's education level, the more likely it is that an individual will experience job change due to automation.[391] The study also found that job automation will disproportionately affect minorities and men.[392] Given the recent job losses incurred across the United States due to COVID-19, it is imperative that the Federal Government invest in job seekers looking to reskill.[393]

Figure 3.7: Comparing Education Level and Potential for Job Change due to Automation



Source: Brookings Institution[394]

[389] $2 million for 340 internships based on a close model of the cybersecurity internship offered at the Department of Homeland Security that offers approximately $5,800 for a 10 week internship. See *Cybersecurity Internship Program*, U.S. Department of Homeland Security (last accessed Sept. 23, 2020), https://www.dhs.gov/homeland-security-careers/cybersecurity-internship-program-0.

[390] Mark Muro, et al., *Automation and Artificial Intelligence*, Brookings Institution at 5 (Jan. 2019), https://www.brookings.edu/wp-content/uploads/2019/01/2019.01_BrookingsMetro_Automation-AI_Report_Muro-Maxim-Whiton-FINAL-version.pdf.

[391] Id. at 42.

[392] Id. at 7.

[393] *The Employment Situation—August 2020*, Bureau of Labor and Statistics (Sept. 4, 2020), https://www.bls.gov/news.release/pdf/empsit.pdf.

[394] Mark Muro, et al., *Automation and Artificial Intelligence*, Brookings Institution at 5 (Jan. 2019), https://www.brookings.edu/wp-content/uploads/2019/01/2019.01_BrookingsMetro_Automation-AI_Report_Muro-Maxim-Whiton-FINAL-version.pdf.

The reskilling of America's workforce is essential for the United States to remain competitive in the global competition for talent. In addition to the many technology jobs that will be required in the next 10 years, "tech adjacent" jobs that require the knowledge to operate and maintain systems will be in high demand as AI and other technologies become ubiquitous.

Recommendation 2.5: Increase Incentives for Public-Private Job Reskilling Training

Congress has already taken some steps to provide greater funding for reskilling by enacting the Strengthening Career and Technical Education for the 21st Century Act (CTE) in 2018.[395] Community colleges have benefited from CTE since monies can be spent on technical training offered at two-year schools. Each state develops a CTE Plan that requires them to consult with various stakeholders (which include community organizations, representatives of business, and industry). CTE also helps deliver professional development, a connection point for internships, and work based opportunities through local partnerships. CTE funds can cover a range of subjects that integrate science, technology, engineering, and mathematics fields, including computer science education, with career and technical education. State and local governments can indicate what training programs they need to support new or emerging fields, including AI and other associated technologies.

In particular, STEM career fields have benefitted from this Act and postsecondary credentials that are recognized by industry are eligible for funding. By endorsing or recommending a spending increase under this act, NSCAI can further improve the quality and quantity of the digital workforce. In addition to STEM, CTE also includes funding for teachers to use technology to teach, including distance learning. The CTE program is currently funded at $1.9 billion.[396] The President's budget request for FY 2021 is $2.7 billion.[397]

Proposed Legislative Branch Action

Congress should support the Strengthening Career and Technical Education for the 21st Century Act by fully funding the FY 2021 request of $2.7 billion for the program.[398]

Issue 3: Microelectronics Education

The United States needs to invest in its ability to recruit and train a microelectronics capable workforce. If it does not, the United States risks losing its ability to meet demand for unique hardware needs, and risks becoming overly reliant on uncleared non-U.S. citizens.

To meet the growing demand for secure microelectronics, the United States needs enduring U.S. citizen workforce development and retention to accomplish four things: 1) ensure access to state of the practice and enable access to state of the art microelectronics technology, 2) secure full lifecycle confidentiality, integrity, verification, validation, and supply chain for

[395] Pub. Law 115-224, Strengthening Career and Technical Education for the 21st Century Act, 132 Stat. 1563 (2018), https://www.congress.gov/bill/115th-congress/house-bill/2353/text.

[396] *Career, Technical, and Adult Education: Fiscal Year 2021 Budget Request*, U.S. Department of Education at N-1 (2020), https://www2.ed.gov/about/overview/budget/budget21/justifications/n-ctae.pdf.

[397] Id.

[398] This figure is based off of the President's FY 2021 budget. See id.

warfighter electronics, 3) develop sustainable sources of U.S. company-owned, U.S.-located mission essential radiation-hardened (rad-hard) electronics capabilities, specialized radio frequency and electro-optic components; 4) and create a secure pipeline for disruptive R&D, transition, supply chain aware technology development, education, and workforce.

Microelectronics is the underlying fabric of the United States warfighting capability. The microelectronics industry has changed dramatically since its birth following World War II. The DoD used to drive the demand for microelectronic features and reliability but is now consistently less than 1 percent of global market demand.[399] The United States Government no longer drives the market which puts the DoD at risk from unreliable suppliers.

The National Defense Strategy outlines five key mission focus areas: 1) Space Offense and Defense; 2) Missile Defense; 3) Nuclear Modernization; 4) Fully Networked Command, Control and Communications; and 5) Cybersecurity. The first four mission focus areas require radiation-hardened (rad-hard) electronics for performance in challenging environments. Maintaining U.S. weapon system lethality against peer competitor nations depends upon technological advances, one of which is incorporation of AI.

In addition to rad-hard electronics, AI systems are increasingly relying on specialized "AI chips" that attain "high efficiency and speed for AI-specific calculations."[400] According to a study conducted by the Center for Security and Emerging Technology:

> *Such leading-edge, specialized "AI chips" are essential for cost-effectively implementing AI at scale; trying to deliver the same AI application using older AI chips or general-purpose chips can cost tens to thousands of times more.*[401]

State-of-the-art AI chips are necessary to cost-effectively deploy cutting edge AI applications across the DoD, which will require a stable and reliable domestic supply chain. Microelectronics designed for AI can also take several forms. For example, the current generation of general use chips like Field Programmable Gate Arrays, Application Specific Integrated Circuits, and Graphics Processing Units can accelerate AI applications and new AI-specific chips are being researched and designed. Each requires a unique set of hardware skills to understand their opportunities, tradeoffs, and vulnerabilities for national security applications.

Since AI applications are inherently fueled by integrated circuits, the demand for trusted, reliable, secure semiconductors is expected to grow dramatically in the coming years. Trusted, reliable, secure electronics must mitigate both maliciously inserted vulnerabilities and any latent vulnerabilities subject to malicious exploitation. In addition, as AI

[399] David Chesebrough, *Trusted Microelectronics: A Critical Defense Need*, National Defense Magazine, (Oct. 31, 2017), https://www.nationaldefensemagazine.org/articles/2017/10/31/trusted-microelectronics-a-critical-defense-need.

[400] Saif Khan & Alexander Mann, *AI Chips: What They Are and Why They Matter*, Center for Security and Emerging Technology at 4 (April 2020), https://cset.georgetown.edu/research/ai-chips-what-they-are-and-why-they-matter/. AI chips also "dramatically accelerate the identical, predictable, independent calculations required by AI algorithms. They include executing a large number of calculations in parallel rather than sequentially, as in CPUs; calculating numbers with low precision in a way that successfully implements AI algorithms but reduces the number of transistors needed for the same calculation; speeding up memory access by, for example, storing an entire AI algorithm in a single AI chip; and using programming languages built specifically to efficiently translate AI computer code for execution on an AI chip." Id. at 5.

[401] Id. at 3.

technologies become more sophisticated, the resulting increasing volume of data will need to move faster, driving systems to use state-of-the-art electronics.

The Problems

The design and manufacturing of microelectronics in the United States requires a deeply skilled technical workforce. The Commission's recommendations are an example of how to improve the United States' microelectronics footing in terms of expertise, but is not a comprehensive solution to the issue. The Commission offers steps to foster a capable workforce in both the private and public sectors, recognizing that the demand for microelectronics talent in the private sector far exceeds the demand within government.

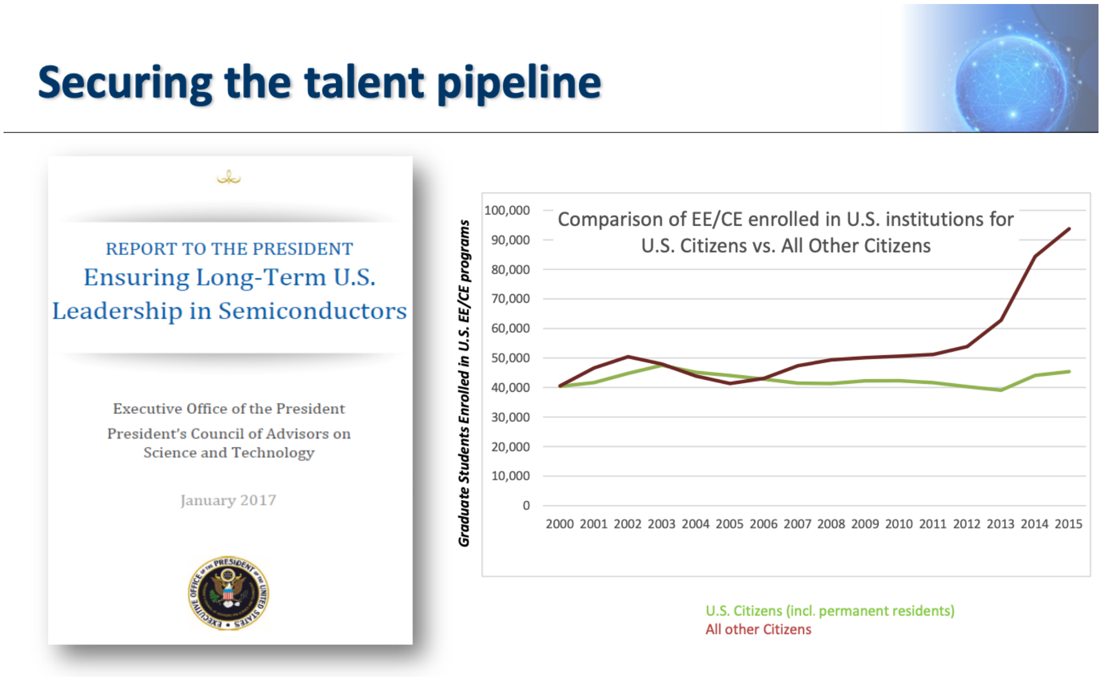
This lack of U.S. citizen microelectronics capable workforce has created multiple problems within the microelectronics hardware field. First, there is no "best practice" integration across the field to exploit AI research specifically for DoD missions. Thus, it is highly likely that redundancies in research will expend precious AI R&D funding that will also erode the United States' current strategic advantage in this field.

Second, there is not a clear path for talent development to bring U.S. citizen students and practitioners into the design and development of systems that are required for national security. Bringing students and practitioners into government service has the additional issue that government salaries are not competitive when compared to compensation in the private sector.

Third, the ratio of U.S.-born versus foreign-born students enrolled in electrical and computer engineering, physics, materials science & engineering, and nuclear engineering degree programs is decreasing. In 2015, nearly 45,000 more foreign-born students studied electrical engineering (EE)/computer engineering (CE) in American universities than Americans.[402] The United States is educating microelectronics workforces of the world, but participating students are overwhelmingly foreign-born. This limits the pool of researchers in this area that can receive a security clearance for classified microelectronics work.

[402] Victoria Coleman, et al., *Microelectronics*, Defense Science Board Quick Task Force on Technology Strategy at 27 (Dec. 10, 2019). See also *Ensuring Long-Term U.S. Leadership in Semiconductors*, President's Council of Advisors on Science and Technology (Jan. 2017), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf; *2020 National Science Board Science and Engineering Indicators: The State of U.S. Science and Engineering*, National Science Board (Jan. 2020), https://drive.google.com/file/d/1MwkKm9f2r13o9G6tWEdhPcsNxxoms9Ou/view?usp=sharing.

Figure 3.8: Securing the Talent Pipeline



Securing the talent pipeline

REPORT TO THE PRESIDENT
Ensuring Long-Term U.S. Leadership in Semiconductors

Executive Office of the President
President's Council of Advisors on Science and Technology

January 2017

Source: Defense Science Board[403]

Fourth, training for such a microelectronics capable workforce is also a long, time-intensive process. Exacerbating this issue, changes within the microelectronics field happen at such a quick pace that learning is a continual process in order to stay relevant in the field.

The DoD will soon face major shortcoming in its microelectronics capable workforce.[404] If the United States does not aggressively address the projected gaps in the microelectronics workforce, it will find itself at a competitive disadvantage in the near future.

The Benefits of a United States based Microelectronics Capable Workforce

Expanding the pool of microelectronics experts broadly while also creating a dedicated pipeline of engineers within the national security space has many benefits. Providing training to microelectronics experts who go into industry will build on the nation's existing private sector strengths in electronic design and semiconductor manufacturing equipment. It will also expand the potential pool of workers for establishing leading edge manufacturing capabilities within the United States. Finally, a dedicated pipeline of microelectronics engineers in the United States provides a secure way to meet DoD's growing needs while providing the students in the program with an assured, stable career path.

[403] Victoria Coleman, et al., *Microelectronics*, Defense Science Board Quick Task Force on Technology Strategy at 6 (Dec. 10, 2019).

[404] *Team 1 White Paper: Future Needs & System Impact of Microelectronics Technologies*, NDIA Trusted Microelectronics Joint Working Group at 2 (July 2017), https://www.intrinsix.com/hubfs/Premium_Content/trusted-asic-design/Future_Needs_and_System_Impact_of_Microelectronics_Technologies.pdf.

To counter the first problem, development of workforce curricula, establishing the pipeline creates a need for an overarching integrated solution. The workforce development and education program can focus efforts on promising R&D, while reducing unnecessary redundancy—through the process of funds allocation. Funding decision makers will decide how much overlap and duplication is healthy.

Countering the second problem, there is immense pride in providing for the defense of the United States, a sense of patriotism shared widely within private industry as well as within the government. The United States must build a microelectronics workforce of U.S. citizens for private industry as well as the government. Government employee access to the latest technologies is essential: as weapon systems are transformed for the shift to peer competitors, their foundational microelectronics must be state-of-the-art.

Countering the third problem, an enduring U.S. based microelectronics workforce education and development program, will draw talented U.S. citizen EE/CE participants. There are millions of young video-game players and unmanned aerial vehicle flyers who thrive on high-performing technologies to give them competitive advantage over their peers. Transforming that mentality to a passion for high tech microelectronics that give the country advantage over its competitors can lead to a successful workforce pipeline of U.S.-born EE/CE enthusiasts.

The fourth problem is inherently solved by funding universities and colleges to push the technology R&D envelope—which faculty and research staff already want. Often the limiting factors are not passion and creativity and understanding and knowledge, but funding. With assured future R&D and education and development funding, faculty and staff are free to pursue technological advances rather than seeking funding. Secure funding streams facilitate flexibility and projects can be varied to keep up with the pace of changing trends throughout the microelectronics world.

In summary, a sustained flow of U.S-born microelectronics capable talent will ensure the delivery of secure microprocessors for DoD applications and give the U.S an edge in the global race for microelectronics talent. The country that can attract, educate, develop, and retain the top minds will maintain the international advantage in technological progress. Timing is critical. While the United States appears to still maintain a global lead in educating and attracting the world's top AI talent, the improving quality of Chinese institutions, their robust pipeline of science and engineering graduates, and plentiful funding for research hold the potential to shift this position in the coming years—if not sooner.

Recommendation 2.6: Create a scalable and replicable microelectronics capable workforce development model

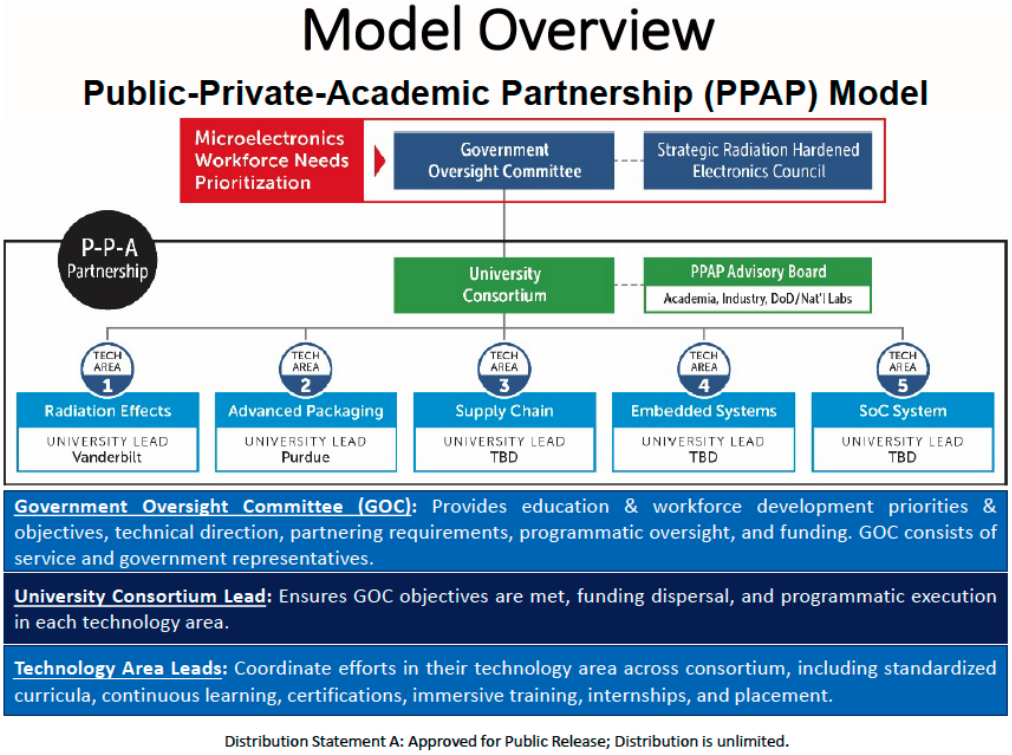
This option was developed by the Strategic Radiation Hardened Electronics Council (SRHEC), for which Naval Surface Warfare Center/Crane, is the Technical Execution Lead, in partnership with Purdue University, Vanderbilt University, and other United States Government interagency partners to provide a reliable, sustained pipeline of microelectronics capable workforce talent to the private sector—especially the aerospace and defense industry—and the United States government. This model is meant to integrate a national approach to learning objectives that drive curriculum, pioneer engineering education expertise to refine standards and drive consistency and allows partners to scale and replicate the model quickly and effectively. This consortium-based approach integrates and aligns aspects that historically have existed independently—research, internships, curriculum, and career pathways. This approach also enables a national program with a regional focus to meet government and industrial workforce needs. Finally, this approach will provide sustained funding for faculty members to establish research clusters to provide long-term opportunities for student researchers.[405]

Systematic Public-Private-Academic Partnership (PPAP) involvement will ensure insights and awareness of microelectronics innovation from all perspectives, and serves as a cost sharing model. Ongoing collaboration of academia, industry, and government within the PPAP Advisory Board will identify future workforce needs that are provided as input to the Government Oversight Committee for prioritization.[406] The PPAP is designed to ensure the curricular plans are based on the right requirements and to advance knowledge sharing in the larger ecosystem. The consortium aspect of this model construct—with a Consortium Manager, joint advisory board, and university consortium verticals—is explicitly designed to enable scale (to other universities) and replication (to additional microelectronics or other DoD technology areas) and to facilitate knowledge sharing within the consortium membership. The Consortium Manager will lead the continuous effort to recruit industry partners and academic consortium members in existing technical areas or new technology verticals in collaboration with government leadership. The Consortium Manager and joint advisory board provide across-the-board integration and prioritization so workforce development fills existing gaps identified through the SRHEC processes.

[405] It is important to note that this PPAP workforce model is being executed by the Navy in support of the OSD T&AM program making it an OSD-led effort.

[406] See Figure 3.9 below. Material for this option was provided by Purdue University and The Strategic Radiation Hardened Electronics Council, for which Naval Surface Warfare Center/Crane, is the Technical Execution Lead. For the sake of clarity, the acronym PPAP and PPA are interchangeable.

Figure 3.9: Public-Private-Academic Partnership Model



Model Overview

Public-Private-Academic Partnership (PPAP) Model

Microelectronics Workforce Needs Prioritization

Government Oversight Committee

Strategic Radiation Hardened Electronics Council

P-P-A Partnership

University Consortium

PPAP Advisory Board

Academia, Industry, DoD/Nat'l Labs

TECH AREA 1 Radiation Effects UNIVERSITY LEAD Vanderbilt

TECH AREA 2 Advanced Packaging UNIVERSITY LEAD Purdue

TECH AREA 3 Supply Chain UNIVERSITY LEAD TBD

TECH AREA 4 Embedded Systems UNIVERSITY LEAD TBD

TECH AREA 5 SoC System UNIVERSITY LEAD TBD

Government Oversight Committee (GOC): Provides education & workforce development priorities & objectives, technical direction, partnering requirements, programmatic oversight, and funding. GOC consists of service and government representatives.

University Consortium Lead: Ensures GOC objectives are met, funding dispersal, and programmatic execution in each technology area.

Technology Area Leads: Coordinate efforts in their technology area across consortium, including standardized curricula, continuous learning, certifications, immersive training, internships, and placement.

Distribution Statement A: Approved for Public Release; Distribution is unlimited.

Source: Alison Smith & Matthew Kay[407]

This prototype microelectronics capable workforce development model will provide an immersive education program with DoD-relevant research and internships integrated with curriculum learning. Collaborative working agreements among the nation's premier universities within each disciplinary field will guarantee multi-institutional and multi-disciplinary research opportunities for each degree level, which can only happen if faculty have access to R&D funding as discussed above. A curriculum immersed in preprogrammed research and internship paths will be seen as an attractive option for students.

At a minimum, $24.47 million per year over the next decade of additional funds are needed to address each critical technical area—$122.36 million per year over the next decade of additional funds are needed to initiate a parallel AI-specific consortium, which could be executed beginning in FY 2022.[408] Without these additional funds, the program would not address key workforce capabilities at the intersection of AI and microelectronics. This option would tentatively produce 91 graduates a year with B.S., M.S., or Ph.D. per technical vertical (455 graduates per year for all verticals).[409]

[407] Graphic provided to NSCAI by Alison Smith, Trusted & Assured Microelectronics Education & Workforce Development Co-Lead, OUSD(R&E) and Matthew Kay, Trusted & Assured Microelectronics DoD Unique Needs Project Lead, OUSD(R&E)/(RT&L).

[408] *Asymmetric Workforce Initiative for Microelectronics Needs* (Mar. 4, 2020) (provided to NSCAI by Alison Smith, Trusted & Assured Microelectronics Education & Workforce Development Co-Lead, OUSD(R&E) and Matthew Kay, Trusted & Assured Microelectronics DoD Unique Needs Project Lead, OUSD(R&E)/(RT&L)).

[409] Id.

Proposed Legislative Branch Action

Congress should authorize and fully fund the existing PPAP program in FY 2021 and expand it to include an AI-specific consortium in FY 2022.

Recommendation 2.7: Create a National Microelectronics Scholar Program.

To address the microelectronics capable workforce issue, a 2019 study conducted by the Defense Science Board suggested a scholar program similar to the SMART program.[410] SMART would serve as a representative framework for a new comprehensive National Microelectronics Scholarship Program (NMSP), but a NMSP would tailor the SMART framework to focus on microelectronics and expand the service obligation from just the U.S.-based labs to domestic companies and government civilian employment.

This option would tentatively produce 750 graduates a year with B.S., M.S., or Ph.D. EE/CE degrees with general goals at each educational step.[411] For Bachelor's degrees, the goal would be creating and maintaining the pipeline of talent who could be identified as capable of microelectronics work. The Master's degree students would be incentivized to pursue advanced study and U.S. national Ph.D. students would be equipped to contribute to the microelectronics workforce at any number of private companies or government positions.

Proposed Legislative Branch Action

Congress should authorize and fully fund a National Microelectronics Scholar Program.

[410] Victoria Coleman, et al., *Microelectronics*, Defense Science Board Quick Task Force on Technology Strategy at 27 (Dec. 10, 2019).
[411] See id.

TAB 4 — Protect and Build Upon U.S. Technology Advantages

Artificial Intelligence (AI) exists within a constellation of emerging technologies. As the Commission stated in its *2019 Interim Report*, "[d]evelopments in AI amplify and reinforce other technologies (and vice versa), underscoring the importance of supporting progress across the board."[412] While AI is the lynchpin of this constellation given its ability to enable or be enabled by such a wide variety of technologies, their interconnected nature is why the Commission's mandate includes AI and "associated technologies." The four "associated technologies" that enable or are enabled by AI which the Commission believes present the most pressing strategic risks and opportunities are microelectronics, 5G telecommunications, quantum computing, and biotechnology. It is imperative that the United States continue posturing itself for a sustained technology competition that extends beyond AI and encompasses a broader suite of associated, emerging technologies.

U.S. efforts to ensure leadership in AI do not exist in a vacuum. Each of these associated technologies used in conjunction with AI poses unique national security challenges and opportunities, a fact which has not escaped the attention of U.S. competitors. China in particular has made significant investments in AI and biotechnology, and has been transparent with its intentions to combine each with AI to enable new industries and strategic capabilities. The United States must not only seek advantages in the traditional elements of the AI stack (algorithms, data, hardware, and talent), but also invest in enabling technologies such as advanced microelectronics and quantum computing; proactively address new challenges posed by AI-powered breakthroughs in biotechnology; and ensure that its supply chains across all technologies and industries are sufficiently secure and resilient. For example, AI's ability to enhance biotechnology has the potential to dramatically enhance human health and well-being while also creating profound new national security threats, and poses unique challenges due to U.S. competitors' disregard for individual privacy and long-standing bioethical norms. Policymakers must understand and begin to plan for these future challenges today.

Building on the previous recommendations of the Commission, this Tab has four sections.[413] First, it examines how AI can enable advances in biotechnology which pose new national security threats. Second, it discusses how quantum computers can drive advances in AI and the associated national security challenges that arise. Third, it examines developments pertaining to the U.S. microelectronics industry since the Commission released its *First Quarter (Q1) Recommendations* in March 2020, and the state of U.S. supply chains for critical technologies. And fourth, it recommends steps the Executive Office of the President must take now to better organize itself for technology competition, which are a necessary precursor to long-term success. At the end of each section the Commission provides

[412] *Interim Report*, NSCAI at 50 (Nov. 2019), https://www.nscai.gov/reports.

[413] In the Commission's First Quarter Recommendations, NSCAI offered recommendations on microelectronics and 5G, several of which Congress has taken action to adopt. See *First Quarter Recommendations*, NSCAI at 45-62 (Mar. 2020), https://www.nscai.gov/reports.

recommendations on how the United States can adapt to better address challenges associated with each of these fields.

Part I: Biotechnology

Biology is now programmable. Just as computer code contains the data which defines how a program operates, DNA, RNA, and proteins contain the data which defines how living organisms operate. Recent technical advances have made this core biological data readable and editable, enabling human analysis and manipulation of life at its most fundamental level. However, the ability to read and even edit this data currently exceeds the ability to understand it.

AI has already demonstrated an ability to fill this knowledge gap, and given the complexity of the data involved it will be essential to any future efforts to gain a comprehensive understanding of how these basic building blocks of life operate. The resulting scientific breakthroughs, particularly when combined with advances in synthetic biology and genetic editing, will fundamentally transform the biological sciences, driving new innovations that significantly enhance human health and capacity. While some of these projected innovations and discoveries may currently appear fantastical and decades away, advancements in AI, as applied to biotechnology, can rapidly compress timescales and make certain innovations and discoveries a reality in the near future.[414] These technological breakthroughs will also cause the biotechnology sector to become a major driver of overall U.S. economic competitiveness.

However, they will also create novel national security challenges, ranging from engineered pathogens to augmented competitor human physiological or mental capabilities. The United States currently is not postured to address such challenges, and biological threats have rarely been a priority issue for the U.S. national security community. The COVID-19 pandemic clearly illustrates that the United States must think more broadly about national security threats than it has in the past, and that biological threats in particular have the potential to impose significant costs on U.S. society and security.[415]

Additionally, U.S. competitors see the potential for AI to spur new, transformational advances in biotechnology. China in particular is actively seeking global leadership in both fields, sees its AI and biotechnology strategies as mutually reinforcing, and believes the synergies between the two will translate into military advantage.[416] China also faces fewer barriers to collecting, using, and combining human biological data given its disregard for individual privacy and bioethical principles. The global reach of China's genomics giant, BGI, poses similar threats in the biotechnology sector as Huawei does in the communications sector, as the Commission discusses below.

[414] A relevant historical example is the Human Genome Project, which was completed two years ahead of schedule and 10% under budget largely due to advancements in computational capabilities over the course of the study. AI is likely to similarly advance contemporary research, but at an even greater magnitude and scale. See Amy Bennett, *Computers Helped Drive Breakthrough in Human Genome Sequencing*, Computer World (Dec. 8, 2000), https://www.computerworld.com/article/2783707/computers-helped-drive-breakthrough-in-human-genome-sequencing.html.

[415] Regarding COVID-19 specifically, see Jason Matheny, et al., *The Role of AI Technology in Pandemic Response and Preparedness: Recommended Investments and Initiatives*, NSCAI (June 25, 2020), https://www.nscai.gov/reports.

[416] Elsa Kania, *Minds at War: China's Pursuit of Military Advantage through Cognitive Science and Biotechnology*, Prism (Jan. 2020), https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Kania_82-101.pdf.

Given the growing national security nexus, the Commission believes it necessary to examine how AI empowers and enables advances in biotechnology, analyze the specific national security threats that are most concerning in this space, and provide recommendations as to how the United States can better posture itself now to respond to these threats in the future.

How AI Enables Biotechnology and Creates New Opportunities

The lines between biological and computational sciences are increasingly being blurred as biology becomes more reliant on large-scale data analysis. Much like AI, the biological sciences and the biotechnology industry have been revolutionized by significant increases in available computing power and memory. Computational advances have driven new discoveries and given researchers access to significant new quantities of biological data, and applying machine learning to these datasets has generated additional research breakthroughs. As available biodata increases, AI will be key to gaining a more comprehensive understanding of biological functions, and will drive new ways to understand and manipulate biology.

AI has already facilitated significant developments in biotechnology. Computer vision techniques applied to medical imagery have enabled more accurate and efficient diagnoses.[417] Machine learning has improved drug discovery by allowing researchers to more accurately predict which compounds will prove effective before engaging in preclinical or clinical trials, and discover new antibiotics.[418] In January 2020, researchers in the United Kingdom (UK) claimed they had developed a new drug for treating obsessive compulsive disorder which was identified through the use of AI and developed in under a year, contrasted with an estimated 4.5 years had they used traditional statistical techniques.[419]

Genomics

While these improvements are notable, advances in genomics related to AI, namely the significant decrease in cost and increase in availability of genetic data, have the potential to revolutionize the biotechnology industry. Since the Human Genome Project first mapped the entire human genome in 2003, the cost of DNA sequencing has decreased exponentially, from approximately $50 million per human genome then to under $600 today.[420] As a result, the amount of available biodata has exploded over the last ten years, and researchers estimate that by 2025 up to two billion human genomes could be sequenced.[421] Genome sequencing has also grown significantly faster and more precise over this time, and gene editing techniques have given researchers the ability to edit genes more accurately and

[417] Junfeng Gao, et al., *Computer Vision in Healthcare Applications,* Journal of Healthcare Engineering (Mar. 4, 2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5857319/.

[418]Jonathan Stokes, et al., *A Deep Learning Approach to Antibiotic Discovery*, Cell (Apr. 16, 2020), https://www.cell.com/cell/fulltext/S0092-8674(20)30102-1?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS0092867420301021%3Fshowall%3Dtrue.

[419] *Sumitomo Dainippon Pharma and Exscientia Joint Development New Drug Candidate Created Using Artificial Intelligence (AI) Begins Clinical Trial*, Exscientia (Jan. 30, 2020), https://www.exscientia.ai/news-insights/sumitomo-dainippon-pharma-and-exscientia-joint-development.

[420] *The Cost of Sequencing a Human Genome*, National Human Genome Research Institute (Aug. 25, 2020), https://www.genome.gov/about-genomics/fact-sheets/Sequencing-Human-Genome-cost.

[421] Erika Check Hayden, *Genome Researchers Raise Alarm Over Big Data*, Nature (July 7, 2015), https://www.nature.com/news/genome-researchers-raise-alarm-over-big-data-1.17912.

quickly than ever before, further increasing the demand for genetic data and the possibilities for genomics.

AI is extremely well suited to analyzing genetic data, given its complexity and sheer size; a single human genome contains approximately three billion base pairs, and represents about 40 gigabytes of data. AI can facilitate cheaper, easier, and more accurate readings of individual genetic data. In 2017, Google released DeepVariant, an open-source deep learning tool designed to identify genetic mutations in individual DNA sequences and distinguish them from random sequencing errors or benign variations, which outperformed the leading statistical approaches by a factor of ten.[422]

Combining powerful deep learning tools with large databases of genetic information has the potential to be even more revealing. Currently researchers' ability to read DNA significantly exceeds their ability to understand how the genome works. However, with access to sufficient data, deep learning algorithms will allow researchers to much more rapidly identify which genes are associated with specific traits or characteristics and determine how genes interact with one another. If combined with the associated metadata for each sequence, this application of AI has the potential to significantly increase the understanding of the human genome, as well as the genomes of other organisms, giving scientists a complete roadmap of how the genome functions and a better understanding of cancer and rare diseases.[423]

Human, Animal and Agricultural Health

A more nuanced understanding of the human genome could facilitate significant advancements related to human health, including more accurate predictions of individual disease risk, as well as targeted and personalized therapeutics.[424] This has the potential to revolutionize medicine, particularly if combined with synthetic biology and genetic editing, facilitating the creation of drugs uniquely tailored to each individual, alterations to the gut microbiome to improve health outcomes, and eliminating diseases caused by genetic mutations.[425] A McKinsey & Company study published in May 2020 estimated that with anticipated advances in cell, gene, RNA, and microbiome therapies which are conceivable given the science of today, these techniques have the potential to eliminate approximately 45 percent of the total global disease burden.[426] The same techniques used to eliminate genetic diseases could allow for genetic modifications to facilitate cognitive or physiological improvements in humans, although such activity would raise significant bioethical concerns.

[422] Megan Molteni, *Google Is Giving Away AI That Can Build Your Genome Sequence*, Wired (Dec. 8, 2017), https://www.wired.com/story/google-is-giving-away-ai-that-can-build-your-genome-sequence/.

[423] Óscar Álvarez-Machancoses, et al., *On the Role of Artificial Intelligence in Genomics to Enhance Precision Medicine*, Pharmacogenomics and Personalized Medicine (Mar. 19, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7090191/.

[424] Disease prediction in particular has the potential to be enhanced by AI, given that disease prevalence and severity is related to so many variables.

[425] Óscar Álvarez-Machancoses, et al., *On the Role of Artificial Intelligence in Genomics to Enhance Precision Medicine*, Pharmacogenomics and Personalized Medicine (Mar. 19, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7090191/.

[426] Michael Chui, et al., *Executive Summary: The Bio Revolution*, McKinsey Global Institute at 10 (May 13, 2020), https://www.mckinsey.com/~/media/McKinsey/Industries/Pharmaceuticals%20and%20Medical%20Products/Our%20Insights/The%20Bio%20Revolution%20Innovations%20transforming%20economies%20societies%20and%20our%20lives/MGI_The%20Bio%20Revolution_Executive%20summary_May%202020.pdf.

AI also has the potential to drive non-human biological advances stemming from genomics. Deeper analysis of agricultural genomes will allow farmers to better predict crop yields, more effectively breed plants to improve agricultural output, and allow for more granular genome editing to further improve yield in a given climate.[427] Farm animals could also be modified or bred to resist specific damaging diseases.[428]

Synthetic Biology

While genome sequencing has given researchers the ability to better understand the building blocks of life, synthetic biology techniques have begun to make organic matter programmable by manipulating and inserting new genetic code into organisms to alter their function. AI is driving synthetic biology to new levels by automating the experimentation process, shifting synthetic biology from a trial-and-error approach to one based on precise modeling. As synthetic biology researchers increase experimentation and develop expansive, standardized, and shared datasets, AI's impact on synthetic biology will increase.[429] The Defense Advanced Research Projects Agency's (DARPA) Synergistic Discovery and Design (SD2) program is already pursuing efforts to facilitate iterative, data-driven advances in complex systems which cannot be simulated in totality, and specifically is targeting synthetic biology.[430]

The advent of precise, rapid, and inexpensive synthetic biology techniques has implications for not only medical applications such as drug selection and microbiome alteration, as mentioned earlier, but also materials production. Researchers have already been able to redesign microorganisms to produce synthetic materials such as spider silk[431] or animal-free meat products.[432] Over time, synthetic biology techniques have the potential to produce far more exotic materials, such as cleaner fuels or synthetic organs. Ultimately, up to 60 percent of the physical inputs to the global economy could be produced via synthetic biology, so substantial developments in this field have the potential to upend global supply chains.[433]

Overall, AI is a driving force behind many recent breakthroughs in the biological sciences, and this trend is only beginning. Now that biological researchers have access to genetic code at scale, AI will be the key to unlocking its secrets, helping scientists identify genetic correlations and enable analytical discoveries that would be impossible using manual statistical methods. As biological research becomes even more dependent on large datasets,

[427] See *Genetically Engineered Crops: Experiences and Prospects*, National Academies Press (2016), https://www.nap.edu/catalog/23395/genetically-engineered-crops-experiences-and-prospects.

[428] See *Genus Shares Surge on Deal to Market Gene-Edited Pigs in China*, Reuters (May 16, 2019), https://uk.reuters.com/article/us-china-genus-plc/genus-shares-surge-on-deal-to-market-gene-edited-pigs-in-china-idUKKCN1SM121.

[429] See Ian Hayden, *DARPA Awards Ginkgo Bioworks and Transcriptic $9.5M to Bring AI into the Lab*, Synbiobeta (Apr. 12, 2018), https://synbiobeta.com/darpa-awards-ginkgo-bioworks-and-transcriptic/.

[430] See id.; see also *Ginkgo Bioworks, Transcriptic Awarded $9.5M DARPA Contract*, Genome Web (Apr. 12, 2018), https://www.genomeweb.com/applied-markets/ginkgo-bioworks-transcriptic-awarded-95m-darpa-contract#.X0WQ9NNKjlw.

[431] See John Cumbers & Niko McCarty, *New This Ski Season: A Jacket Brewed From Spider Silk*, Synbiobeta (Sept. 3, 2019), https://synbiobeta.com/new-this-ski-season-a-jacket-brewed-from-spider-silk/.

[432] Kim Thomas, How Fake Meat Could Save the Planet, OneZero (Mar. 25, 2019), https://onezero.medium.com/how-fake-meat-could-save-the-planet-70e23b937e7b.

[433] Michael Chui, et al., *The Bio Revolution*, McKinsey Global Institute at 43 (May 13, 2020), https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/the-bio-revolution-innovations-transforming-economies-societies-and-our-lives.

major advances in biotechnology will soon all be dependent on AI. AI is fundamentally redefining the biotechnology field, which in turn will reshape the world we all live in.

National Security Threats from AI-Enabled Biotechnology Advances

As AI drives biotechnology and enables new technical possibilities in the biological sciences, it will also create new national security threats to the United States. These threats can largely be divided into two categories: strategic threats to U.S. competitiveness driven by competitors' advantages in AI-enabled biotechnology, and specific operational threats enabled by AI-enabled biotechnology breakthroughs. Each of these threats are also potential sources of strategic surprise the United States must prepare for now, especially given the demonstrated potential for AI to quickly accelerate advances in biotechnology.

Strategic Threat - The Bioeconomy as a Source of National Power. As AI fuels rapid new developments in the biological sciences and biotechnology becomes a greater driver of the overall world economy, the strategic consequences of ceding leadership in biotechnology will increase significantly. Should competitors make breakthroughs related to human health it could lower their populations' disease incidence and prolong their mortality, and potentially make the United States dependent on competitors for access to advanced medicines or therapeutics.[434] Economically, new biological applications are projected to create $2 to 4 trillion of direct, annual economic impact in the next ten years.[435] And strategically, if competitors were to gain advantages in biotechnology they could utilize synthetic biology techniques to increase their self-sufficiency for key materials by producing them via biologic means.

Each of these areas has the potential to have significant impact on overall U.S. competitiveness, and ceding leadership in any of them would have substantial national security implications. It is therefore critical that the United States maintain leadership in biotechnology writ large, and ensure that competitors do not leap ahead of the United States due to their ability to utilize AI to leverage potential advantages in biodata quantity.

Operational Threat - Engineered Pathogens. The primary biosecurity concern for decades has been the potential impact of deadly pathogens—either natural or manmade—on the U.S. population. While COVID-19 clearly illustrates the havoc that natural pathogens can wreak, advances in biotechnology have increased the ability of adversaries, and potentially non-state actors, to create engineered pathogens, and AI will enhance their understanding of both the specific genetic weaknesses and susceptibilities of the U.S. population, and how to target them. As competitors' access to genetic data increases, including both data at scale as well as potentially data on key targeted individuals, AI will allow the creation of increasingly dangerous and precise engineered pathogens.[436]

[434] Mark Kazmierczak, et al., *China's Biotechnology Development: The Role of US and Other Foreign Engagement*, Gryphon Scientific at 135 (Feb. 14, 2019), https://www.uscc.gov/sites/default/files/Research/US-China%20Biotech%20Report.pdf.

[435] Michael Chui, et al., *The Bio Revolution*, McKinsey Global Institute at 60 (May 13, 2020), https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/the-bio-revolution-innovations-transforming-economies-societies-and-our-lives.

[436] Some of the threats posed by advances in biotechnology are listed in the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community (IC). See Dan Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community*, Office of the Director of National Intelligence at 16 (Jan. 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

As a result, AI could enable the creation of pathogens that only impact select groups such as an ethnic group or even targeted individuals.[437] This precision could remove adversaries' concern of a pathogen impacting their own population, potentially increasing their willingness to use such capabilities. In addition to being engineered to increase lethality beyond what would occur via natural selection, such pathogens could also be designed to stimulate more subtle effects, such as increasing fatigue or increasing disease susceptibility, which would be more difficult to detect but could have substantial long-term effects on a wide population. Alternatively, they could be used to target specific crops that are common in the diets of a given population to threaten food security.

Operational Threat - Human Enhancement. As researchers use AI to determine new genetic correlations between genotype and phenotype and more accurately project the impact of potential alterations to the genome, this will eventually facilitate the physical or genetic enhancement of humans to increase mental or physical capabilities.[438] The magnitude of the impact of genetic alterations to human intelligence is uncertain, but estimates range from one standard deviation (approximately 15 IQ points) to over 100 standard deviations of improvement.[439] Many countries are already researching how to use gene therapy, synthetic biology, and other advancements in biotechnology to grant soldiers enhanced mental or physical capabilities.[440] Should a competitor nation-state engage in widespread and advanced use of this practice, it could put the United States at a strategic disadvantage in key industries, with respect to national security decision making, or even on the battlefield.

While many experiments regarding human enhancement, particularly regarding genetic editing to enhance intelligence or physical capabilities, would run afoul of bioethical norms in the United States and many other developed countries, some U.S. competitors do not share the same ethical guardrails, which could enable them to make unique scientific advances in this field. For instance, in 2018 Chinese scientist He Jiankui genetically altered two twins *in utero* to delete the CCR5 gene to reduce their susceptibility to HIV, creating the first genetically-altered babies; it is possible that the true intention of He's experiments may have been to improve cognition, as studies have demonstrated that deleting the CCR5 gene in mice is linked to substantial cognitive improvement.[441] Although he subsequently faced backlash from both the global scientific community and the Chinese government and was

[437] Sarah Knapton, *World Must Prepare for Biological Weapons that Target Ethnic Groups based on Genetics, Says Cambridge University*, The Telegraph (Aug. 13, 2019), https://www.telegraph.co.uk/science/2019/08/12/world-must-prepare-biological-weapons-target-ethnic-groups-based/.

[438] Rachel Cocker, *This Harvard Scientist Wants Your DNA to Wipe Out Inherited Diseases - Should You Hand It Over?*, The Telegraph (Mar. 16, 2019), https://www.telegraph.co.uk/global-health/science-and-disease/harvard-scientist-wants-dna-wipe-inherited-diseases-should/.

[439] Rachel Cocker, *We Should Not Fear 'Editing' Embryos to Enhance Human Intelligence, Says Leading Geneticist George Church*, The Telegraph (Mar. 16, 2019), https://www.telegraph.co.uk/global-health/science-and-disease/should-not-fear-editing-embryos-enhance-human-intelligence-says/; Stephen Hsu, *Super-Intelligent Humans Are Coming*, Nautilus (Oct. 16, 2014), http://nautil.us/issue/18/genius/super_intelligent-humans-are-coming.

[440] Nilanthan Niruthan, *Beyond Human: Rise of the Super-Soldiers – A Primer*, Small Wars Journal (Aug. 26, 2018), https://smallwarsjournal.com/jrnl/art/beyond-human-rise-super-soldiers-primer.

[441] Antonio Regalado, *China's CRISPR Twins Might Have Had Their Brains Inadvertently Enhanced*, MIT Technology Review (Feb. 21, 2019), https://www.technologyreview.com/2019/02/21/137309/the-crispr-twins-had-their-brains-altered/; David Cyranoski, *Baby Gene Edits Could Affect a Range of Traits*, Nature (Dec. 12, 2018), https://www.nature.com/articles/d41586-018-07713-2.

given a three-year prison sentence for conducting the experiments, speculation exists that the Shenzhen government funded He's work.[442]

The Chinese government has also increased its support for research on genetically altering animals to improve their mental and physical functions. For instance, China has expanded neuroscience research on non-human primates while the United States and Europe have generally decreased such activities.[443] This includes numerous genetic experiments on monkeys associated with cognitive intelligence, including implanting human genes associated with intelligence into monkey embryos in an effort to better understand human brain function.[444] Chinese researchers have also created genetically-altered dogs with twice the muscle mass than they would have had otherwise, techniques which if perfected on humans and applied to soldiers could confer substantial advantages.[445]

Additionally, AI has provided breakthroughs in the ability to read and interpret brainwaves, and will be key to future improvements in brain-machine interface technology. This technology has already been used to allow for control of prosthetic limbs, but over time could be expanded to include significantly more advanced functions that facilitate human enhancement, such as greater sensory, physical, or mental capacities.[446] Although such technology is still nascent, it could provide a substantial strategic advantage to whichever country leads in its development given its potential to transform the way humans and machines interact. It is essential that the United States stay at the cutting edge of this field, and also define the field's ethical norms and standards before such devices emerge into the mainstream.

AI applied to large numbers of genetic datasets will both help countries willing to pursue such work better understand brain function without conducting large-scale, internationally-condemned human trials, and ultimately enable human enhancements, which could provide substantial strategic advantages, albeit not in the near term.

U.S. and Competitor Postures on Applying AI to Biotechnology

United States. The United States has a robust biotechnology ecosystem across all elements of research and development.[447] U.S. biotechnology firms and academic institutions have long been at the field's cutting edge, have among the world's best talent, and many are already utilizing AI to facilitate new biotechnology breakthroughs. Additionally, over half of the world's venture capital-funded startups related to both AI and biology are located in the

[442] Austin Ramzy & Sui-Lee Wee, *Scientist Who Edited Babies' Genes Is Likely to Face Charges in China*, New York Times (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/world/asia/china-gene-editing-babies-he-jiankui.html.

[443] Antonio Regalado, *Chinese Scientists Have Put Human Brain Genes in Monkeys—and Yes, They May Be Smarter*, MIT Technology Review (Apr. 10, 2019), https://www.technologyreview.com/2019/04/10/136131/chinese-scientists-have-put-human-brain-genes-in-monkeysand-yes-they-may-be-smarter/.

[444] Elsa Kania, *Minds at War: China's Pursuit of Military Advantage through Cognitive Science and Biotechnology*, Prism at 90 (Jan. 2020), https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Kania_82-101.pdf.

[445] Antonio Regalado, *First Gene-Edited Dogs Reported in China*, MIT Technology Review (Oct. 19, 2015), https://www.technologyreview.com/2015/10/19/165740/first-gene-edited-dogs-reported-in-china/.

[446] *Nonsurgical Neural Interfaces Could Significantly Expand Use of Neurotechnology*, DARPA (Mar. 16, 2018), https://www.darpa.mil/news-events/2018-03-16.

[447] *Safeguarding the Bioeconomy*, National Academies Press (2020), https://www.nap.edu/catalog/25525/safeguarding-the-bioeconomy.

United States, with over $2.5 billion invested in these firms in 2018.[448] The heterogeneous nature of the U.S. population also makes U.S. genetic data very valuable, as it enables researchers to test the impact of hypotheses across racial and ethnic groups relatively easily. The United States has the resources and capability to leverage its advantages in AI to further its existing leadership in biotechnology, spur continued technological breakthroughs, and protect itself from emerging national security threats.

However, the United States also faces some key structural disadvantages that could cause its leadership to erode. First, the United States Government has historically not prioritized biotechnology advances as a pressing national security issue. U.S. biosecurity efforts have predominantly focused on biothreats pertaining to natural or engineered pathogens, and not how rapid, AI-enabled advances in biotech could allow competitors to leapfrog the United States and fundamentally undermine U.S. competitiveness. Prior to COVID-19, biotechnology and biosecurity issues have gone through boom and bust cycles in the U.S. national security community, with intense focus after the 2001 anthrax attacks quickly dissipating.[449] Moreover, almost all departments and agencies in the U.S. national security apparatus have a dearth of talent in the biological sciences, let alone people who have an understanding of both biology and AI.

Additionally, the disaggregated nature of U.S. healthcare data presents significant challenges in a field which is increasingly dependent on large quantities of standardized data. The "All of Us" initiative, created by the National Institute of Health in 2015, is a promising effort that seeks to collect comprehensive genetic and health data on one million U.S. residents to accelerate precision medicine, but took nearly three years to begin enrolling subjects and will likely not meet its enrollment goals until 2024.[450] Second, the United States does not have a comprehensive national strategy for biotechnology, which limits its ability to highlight national security concerns or needs pertaining to biotechnology to the research and commercial community in a systematic way and proactively address future threats.

China. China has emerged as a true global competitor in biotechnology, and has a comprehensive strategy to become the global leader in the field. Biotechnology features prominently in both its 13th Five-Year-plan and Made in China 2025, and it has labeled biotechnology as a key industry for China's long-term competitiveness.[451] Chinese military writings have also increasingly highlighted biology as a new domain of warfare and specifically pointed to the intersection of biology with AI and other technologies as likely to drive future advances in weapons development.[452] The Chinese government also sees AI-enabled advances in biotechnology as critical to addressing some of its significant challenges related to human health and the environment, and enabling it to become a world leader in

[448] NSCAI staff interview (Sept. 16, 2019).
[449] See Susan West Marmagas, *Public Health's Response to a Changed World: September 11, Biological Terrorism, and the Development of an Environmental Health Tracking Network*, American Journal of Public Health (Aug. 2003), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1447942/.
[450] Heather Landi, *NIH All of Us Project Tops 270,000 Sign-Ups and On Track to Enroll 1M Participants by 2024*, Fierce Healthcare (Aug. 16, 2019), https://www.fiercehealthcare.com/tech/nih-all-us-project-tops-270-000-sign-ups-goal-enrolling-1m-participants-by-2024.
[451] Adolfo Arranz, *Betting Big on Biotech*, South China Morning Post (Oct. 09, 2018), https://multimedia.scmp.com/news/china/article/2167415/china-2025-biotech/index.html.
[452] Elsa Kania, *Minds at War: China's Pursuit of Military Advantage through Cognitive Science and Biotechnology*, Prism at 91 (Jan. 2020), https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Kania_82-101.pdf.

agriculture and pharmaceutical production.[453] In 2016 it launched a $9.2 billion precision medicine initiative, the largest in the world, with the goal to sequence 100 million human genomes by 2030.[454]

Although China's biotech industry is still approximately one tenth the size of the U.S. biotech industry, it is growing rapidly due to a significant increase in government support for early-stage biotech companies as well as support to industry leaders.[455] Chinese biotechnology firms have also received heavy investment from its large AI companies. Tencent invested roughly $200 million in iCarbonX, the largest Chinese healthcare startup, which aggregates genetic and health information and uses AI to provide personalized, predictive health recommendations.[456] Baidu is attempting to raise $2 billion to create a biotech startup focused on using AI for drug discovery and disease diagnosis.[457] The Chinese government is also using illicit tactics to provide support to the industry, as Chinese hackers and predatory investors have aggressively targeted data from U.S. biotechnology and healthcare firms, to include both data on specific projects such as COVID-19 vaccine research and general genetic or healthcare data on U.S. persons.[458]

In particular, China has focused extensively on genomics. BGI (formerly named the Beijing Genomics Institute) is China's de facto national champion in the field, and is one of the world leaders in genome sequencing services and machine production, along with the U.S.-based Illumina, as well as in genetics research. BGI has benefited from substantial support from the Chinese government, as well as its 2013 acquisition of a competing U.S. firm, Complete Genomics.[459] It claims it will drive down the cost of DNA sequencing to $100 in 2020, which would represent a six-fold decrease over the current cost.[460]

[453] Notably, cancer is the leading cause of death in China and its cancer mortality rate is 40% higher than that of the United States. See Rui-Mei Feng, *Current Cancer Situation in China: Good or Bad News from the 2018 Global Cancer Statistics?*, Cancer Communications (Apr. 29, 2019), https://cancercommun.biomedcentral.com/articles/10.1186/s40880-019-0368-6#:~:text=Compared%20to%20the%20USA%20and,and%20have%20relatively%20poorer%20prognoses. Regarding China's interest in becoming an agriculture leader, see Amy R. Beaudreault, *China's Growing Power for a Food Secure World*, CSIS (Jan. 8, 2020), https://www.csis.org/analysis/chinas-growing-power-food-secure-world.

[454] David Beier & George Baeder, *China Set to Accelerate Life Science Innovation*, Forbes (Jul. 6, 2017), https://www.forbes.com/sites/realspin/2017/07/06/china-set-to-accelerate-life-science-innovation/#2b4def60e73b.

[455] Mark Kazmierczak, et al., *China's Biotechnology Development: The Role of US and Other Foreign Engagement*, Gryphon Scientific at 2-3 (Feb. 14, 2019), https://www.uscc.gov/sites/default/files/Research/US-China%20Biotech%20Report.pdf.

[456] David Ewing Duncan, *Can AI Keep You Healthy?*, MIT Technology Review (Oct. 3, 2017), https://www.technologyreview.com/2017/10/03/67827/how-ai-will-keep-you-healthy/; David Cyranoski, *Chinese AI Company Plans to Mine Health Data Faster than Rivals*, Nature (Jan. 10, 2017), https://www.nature.com/news/chinese-ai-company-plans-to-mine-health-data-faster-than-rivals-1.21258.

[457] Yingzhi Yang & Brenda Goh, *Exclusive: Baidu, Investors in Talks to Raise $2 Billion for Biotech Startup - Source*, Reuters (Sept. 9, 2020), https://www.reuters.com/article/us-china-baidu-biotech-exclusive-idUSKBN2600UH.

[458] Julian Barnes, *U.S. Accuses Hackers of Trying to Steal Coronavirus Vaccine Data for China*, New York Times (July 21, 2020), https://www.nytimes.com/2020/07/21/us/politics/china-hacking-coronavirus-vaccine.html; see also David Lynch, *Biotechnology: the U.S.-China Dispute Over Genetic Data*, Financial Times (July 31, 2017), https://www.ft.com/content/245a7c60-6880-11e7-9a66-93fb352ba1fe.

[459] In 2010 BGI received a $1.5 billion loan from the state-run China Development Bank. The precise extent of government subsidies to BGI are unknown, but likely substantial. See Kirsty Needham, *Special Report: COVID Opens New Doors for China's Gene Giant*, Reuters (Aug. 5, 2020), https://www.reuters.com/article/us-health-coronavirus-bgi-specialreport/special-report-covid-opens-new-doors-for-chinas-gene-giant-idUSKCN2511CE.

[460] Antonio Regaldo, *China's BGI Says It Can Sequence a Genome for Just $100*, MIT Technology Review (Feb. 26, 2020), https://www.technologyreview.com/2020/02/26/905658/china-bgi-100-dollar-genome/.

BGI has also greatly expanded its research efforts in recent years, transforming itself from a sequencing specialist into a full-stack powerhouse in genomics. It has partnerships with a number of U.S. companies and universities, including the University of Washington and Washington State University.[461] BGI's headquarters in Shenzhen has also become a hub for genetics research, and has specifically funded research into the links between genetics and human intelligence. BGI created the Cognitive Genomics Lab in 2011, which sought to sequence the genomes of over 2,000 genius-level individuals and compare them with a control group to identify the genetic basis for human intelligence.[462]

There are indications that BGI's links with the Chinese government may run deeper than it publicly claims. It built and operates China National GeneBank, the Chinese government's national genetic database.[463] BGI's bioinformatics research has used supercomputers from the People's Liberation Army's (PLA) National University of Defense Technology to process genetic information for biomedical applications, and its researchers have collaborated with PLA researchers on multiple publications.[464] Chinese diplomats have increasingly pushed BGI-built COVID-19 testing kits, including in the United States, and the company has sold 35 million kits to 180 countries, and also built 58 testing labs in 18 countries.[465] In June 2020, the Department of Commerce added two subsidiaries of BGI to the Entity List, accusing them of "conducting genetic analysis used to further the repression of Uighurs and other Muslim minorities."[466]

Additionally, BGI stores much of the data from its gene sequencers on Huawei's cloud computing service, a fact that illustrates some notable similarities between the two firms.[467] Both Huawei and BGI have created platforms capable of collecting significant quantities of sensitive data originating from outside China; communications in one case, genetic information in the other. Both firms have opaque organizational structures that could hide true sources of funding or the scope of their work, both are known to work directly with the Chinese government, and both are subject to the same Chinese cybersecurity law which would compel them to share any data the government requests.[468] And AI will be critical to analyzing, utilizing, and benefiting from the data which both firms collect.

[461] Megan Molteni, *A Chinese Genome Giant Sets Its Sights on the Ultimate Sequencer*, Wired (May 18, 2017), https://www.wired.com/2017/05/chinese-genome-giant-sets-sights-uitimate-sequencer/.

[462] Ed Yong, *Chinese Project Probes the Genetics of Genius*, Nature (May 14, 2013), https://www.nature.com/news/chinese-project-probes-the-genetics-of-genius-1.12985.

[463] *China National Genebank Officially Opens*, BGI (Sept. 22, 2016), https://www.bgi.com/us/company/careers/china-national-genebank-officially-opens/.

[464] Elsa Kania & Wilson Vorndick, *Weaponizing Biotech: How China's Military Is Preparing for a 'New Domain of Warfare'*, Defense One (Aug. 14, 2019), https://www.defenseone.com/ideas/2019/08/chinas-military-pursuing-biotech/159167/.

[465] See Kirsty Needham, *Special Report: COVID Opens New Doors for China's Gene Giant*, Reuters (Aug. 5, 2020), https://www.reuters.com/article/us-health-coronavirus-bgi-specialreport/special-report-covid-opens-new-doors-for-chinas-gene-giant-idUSKCN2511CE; see also Jeanne Whalen & Elizabeth Dwoskin, *California Rejected Chinese Company's Push to Help with Coronavirus Testing. Was That the Right Move?*, Washington Post (July 2, 2020), https://www.washingtonpost.com/business/2020/07/02/china-bgi-california-testing/.

[466] David Shepardson, *Chinese Genetics Company BGI Denies U.S. Human Rights Accusations*, Reuters (July 21, 2020), https://www.reuters.com/article/us-usa-china-human-rights/chinese-genetics-company-bgi-denies-u-s-human-rights-accusations-idUSKCN24N00A.

[467] See Kirsty Needham, *Special Report: COVID Opens New Doors for China's Gene Giant*, Reuters (Aug. 5, 2020), https://www.reuters.com/article/us-health-coronavirus-bgi-specialreport/special-report-covid-opens-new-doors-for-chinas-gene-giant-idUSKCN2511CE.

[468] Matthew Campbell & Dong Lyu, *China's Genetics Giant Wants to Tailor Medicine to Your DNA*, Bloomberg Businessweek (Nov. 13, 2019), https://www.bloomberg.com/news/features/2019-11-13/chinese-genetics-giant-bgi-wants-to-tailor-medicine-to-your-dna.

Finally, China's relative lack of ethical constraints and disregard for individual privacy will give it particular advantages over the United States in the biotechnology space. Chinese scientists' willingness to aggressively push, or exceed, bioethical boundaries could result in China gaining expertise in areas of genetics that the United States is unwilling to pursue. Additionally, China's surveillance apparatus will give it both the incentive to create massive genetic databases, and the means to compel people to do so. There is already evidence that China is trying to create a DNA database containing information on all 700 million Chinese males.[469] China's resulting advantage in genetic data, which the United States alone will not be able to match, will enhance its ability to use AI to generate new scientific breakthroughs that present new national security challenges for the United States in the coming decades.

Russia. Russia does not have the plans or capability to combine mass data collection and AI to threaten U.S. leadership in biotechnology like China, but it does recognize the growing importance of the field and is unlikely to be restrained in its use of biotechnology in pursuit of national objectives. The Russian biotechnology industry lags behind those of the United States and China, although in 2012 the Russian government released BIO2020, a whole-of-government strategy for improving the Russian biotech industry.[470] State-based research and funding dominates the Russian biotech sector, although specific efforts are largely opaque, and few Russian biotechnology firms are seen as industry leaders.

Russia's long-standing disregard for scientific norms and bioethical principles, in conjunction with its interest in utilizing AI for national security purposes, could increase its willingness to utilize advanced biotechnology developments for nefarious purposes. The Russian government's August 2020 approval of a COVID-19 vaccine which had only been tested on 76 people highlights Russia's high tolerance for risk in this field, and its history of state-sponsored doping programs for international athletic competitions demonstrates its willingness to violate rules and norms in search of greater human performance.[471] Given Russia's willingness to develop and employ novel nerve agents such as Novichok in assassination attempts, it likely would also be willing to utilize synthetic biology to develop equivalent novel biological agents.[472] In 2020, the Department of State expressed concern over Russia's compliance with the Biological Weapons Convention, and raised questions about Russian claims that it had destroyed its biological weapons program.[473]

[469] Sui-Lee Wee, *China Is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment*, New York Times (July 30, 2020), https://www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html.

[470] *Emerging Military Technologies: Background and Issues for Congress*, Congressional Research Service at 20 (Aug. 4, 2020), https://fas.org/sgp/crs/natsec/R46458.pdf.

[471] Alison Abbott, *Researchers Highlight 'Questionable' Data in Russian Coronavirus Vaccine Trial Results*, Nature (Sept. 15, 2020), https://www.nature.com/articles/d41586-020-02619-4.

[472] Richard Perez-Pena, *What is Novichok, the Russian Nerve Agent Tied to Navalny Poisoning?*, New York Times (Sept. 2, 2020), https://www.nytimes.com/2020/09/02/world/europe/novichok-skripal.html.

[473] *2020 Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments (Compliance Report)*, U.S. Department of State (2020), https://www.state.gov/2020-adherence-to-and-compliance-with-arms-control-nonproliferation-and-disarmament-agreements-and-commitments-compliance-report-2/#_Toc43298166.

Recommendation 1.1: Prioritize U.S. Leadership in Biotechnology as a National Security Imperative and pursue Whole-of-Government efforts to support U.S. Biotechnology Advantages and ensure the United States is a World Leader in Ethical Genomic Data Aggregation and Analysis.

The combination of advances in AI and biology have the potential to reshape the global economy for the next century. AI-powered biotechnology will underpin most major scientific breakthroughs related to human health, agriculture, and climate science. The nation which is best able to simultaneously leverage both technologies will have substantial strategic advantages for the foreseeable future, potentially becoming a global leader in pharmaceuticals, reducing its reliance on foreign supply chains, and even ensuring it has a healthier and more capable population. In addition to creating strong economic incentives, these factors also make it a national security imperative that the United States take proactive steps to facilitate long-term U.S. leadership in biotechnology.

This will require a whole-of-government effort, as like many other emerging technologies responsibility for biotech does not rest with any single department or agency. The United States should aggressively promote funding for basic research in biology, and particularly in applications of biology which utilize AI. It must focus more resources on forecasting how AI will enable future biotechnology breakthroughs, both in order to better predict the actions of competitors and to inform U.S. research priorities. And it must continue to cultivate talent, both inside and outside government, and commercial activity at the nexus of these fields in order to ensure continued U.S. leadership. Such efforts will also require a mechanism inside the White House which is empowered to coordinate across the economic, technological, and security issues associated with emerging technologies (see Section 4).

The United States should specifically fund and expand existing efforts which aggregate genetic data in a secure manner and include data about corresponding phenotypes, in order to enhance the ability of U.S. researchers to utilize AI to facilitate large-scale biotechnology research and innovation. Examples could include increasing funding for public data resources such as the U.S. national gene bank, GenBank, to allow it to bolster and standardize its datasets. Expanding and accelerating the All of Us initiative, which includes strict privacy safeguards and only shares de-identified data with researchers, could also help grow U.S. biomedical research advantages, and would greatly improve access to high-quality genetic data with the corresponding metadata for phenotype mapping. The United States should also encourage allies and partners to fund similar initiatives in their own countries, and explore efforts to pool these resources. Such investments are critical to ensure that U.S. researchers are not reliant on BGI or other Chinese entities for access to large-scale genomic databases for research.

In addition, the United States should invest in AI techniques and health datasets which would allow more rigorous analysis with fewer samples, as well as better protection of privacy. The United States will always be at a data quantity disadvantage compared to China, particularly with respect to genetic information. China has more people to draw from, greater centralized government control, and the means to either compel people to provide genetic information to centralized databases or deceive them into doing so. As a result, if data quantity ends up driving AI-enabled biotechnology research advantages, the United States will likely cede leadership in the field to China.

To counteract this emerging challenge, the United States should pursue research into AI techniques that are less reliant on data to identify correlations, potentially leveraging its advantages in compute resources to facilitate such work. It should also double down on investments in research on privacy-preserving computational techniques, which would enable researchers to better aggregate and analyze genetic data without putting the privacy of individuals at risk. For instance, advances in homomorphic encryption would enable U.S. researchers to analyze health data while keeping it in an encrypted form, which would facilitate easier storage, sharing, and analysis of health data while also better protecting patient privacy.

Finally, it will also be important to prevent and deter adversaries from illicitly obtaining the private genetic and health data of U.S. persons. The Foreign Investment Reform and Review Act (FIRRMA) of 2018 took some important steps to increase the Committee on Foreign Investment in the United States' (CFIUS) authority to review transactions that would provide foreign investors with access to sensitive U.S. datasets. However, more work remains to be done to close loopholes in FIRRMA pertaining to emerging technologies.[474]

Recommendation 1.2: Increase the Profile of Biosecurity Issues and Biotechnology Competition within the U.S. National Security Departments and Agencies, treat Chinese Advancements in Biotechnology as a National Security Priority, and update the U.S. National Biodefense Strategy to include a Wider Range of Biological Threats.

The United States must treat China's attempts to gain strategic advantage by leveraging AI to achieve breakthroughs in biotechnology as a national security priority. While there are many fields in which AI will prove transformative, rapid advancements in biotechnology enabled by AI have the potential to systematically change the global economy and the strategic landscape, posing both specific and systemic national security threats. Such developments are all reliant on both large quantities of data and world-class AI capabilities to analyze that data. The Chinese government's significant financial support for both the AI and biotechnology sectors, its advantages in biodata collection, and its willingness to ignore or violate bioethical norms and principles, as well as the PLA's expressed interest in the military applications of AI-enabled biotechnology, are cause for substantial concern. China's strategies to become the world leader in both fields are mutually reinforcing, so observing developments related to either China's AI strategy or its biotechnology strategy in isolation will miss the bigger picture.

The United States must increase the profile of and resources devoted to biosecurity and biotechnology issues in all U.S. national security departments and agencies. It must proactively monitor ways in which the Chinese government and key Chinese firms intend to utilize AI to spur innovations in biotechnology which have relevance to U.S. national security, particularly with respect to human genetic enhancement or pathogen engineering, or which would create new U.S. supply chain vulnerabilities. These issues can no longer be a

[474] For additional details about potential reforms to CFIUS pertaining to emerging technologies, see *Second Quarter Recommendations*, NSCAI at 75 (July 2020), https://www.nscai.gov/reports.

national security afterthought only considered by a small number of biodefense specialists, given their centrality to the current and future geostrategic competition.

As a first step, the United States should update its *National Biodefense Strategy*, which currently only focuses on natural or engineered pathogens, to include a wider vision of biological threats.[475] The strategy should specifically examine how AI could enable new biological advances which pose unique national security threats, such as human enhancement, and how U.S. competitors could utilize advantages in biotechnology or biodata as an instrument of national power. It should also specifically consider how AI could identify and counter the creation of advanced, engineered pathogens which target certain elements of the U.S. population or food supply. AI is facilitating a rapid evolution of the biotechnology field, and the U.S. biodefense strategy must evolve with it.

The United States should also ensure that senior advisory boards focused on emerging technologies and national security have a sufficient level of expertise on biotechnology issues. Boards such as the Defense Innovation Board, the Defense Science Board, the President's Council of Advisors on Science and Technology, and the JASON Defense Advisory Panel should ensure at least twenty percent of their experts have demonstrated experience in biology, medicine, pharmaceutical sciences, or related fields. These boards have traditionally emphasized physics and information technology fields to a greater degree than biology, and could be important vehicles for raising the profile and providing analysis of biotechnology issues to senior leaders inside the government.

Recommendation 1.3: Launch a Strategic Communications Campaign to Highlight BGI's Links to the Chinese Government and How China is Utilizing AI to enable Ethically Problematic Developments in Biotechnology and Strengthen International Bioethical Norms and Standards regarding Genomics Research.

The United States should take a more aggressive public posture regarding BGI—China's de facto national champion in genetic sequencing and research—and publicly highlight its links to the Chinese government and the national security risks that the company poses to the United States and its allies. BGI may be serving, wittingly or unwittingly, as a global collection mechanism for Chinese government genetic databases, both providing China with greater raw numbers and diversity of human genome samples, as well as access to sensitive personal information about key individuals around the world. The highest levels of the United States government should publicly state these concerns so as to raise awareness among the U.S. commercial and academic biotechnology communities, as well as U.S. allies, many of which currently have partnerships or business dealings with BGI. The United States should also warn BGI and the Chinese government that it will closely monitor BGI's activities, and should BGI either be utilized as a mass DNA collection apparatus for the Chinese government or directly facilitate mass surveillance inside China or overseas, it could face additional U.S. regulatory action. Additionally, the United States should more aggressively highlight and condemn ethically problematic AI-enabled biotechnology research

[475] *National Biodefense Strategy*, The White House (2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf.

or applications by the Chinese researchers or the Chinese government, such as research into human enhancement or systematic and forced collection of DNA samples.

Simultaneously, the Departments of State and Health and Human Services, in conjunction with U.S. industry and academia, should lead global efforts to emphasize and further define the bioethical guardrails for experiments involving AI applied to genetics and synthetic biology in particular. Doing so would have two effects: 1) it would increase public pressure on Chinese and other researchers to refrain from engaging in such problematic experiments, potentially deterring China and other competitors' pursuit of certain strategic but highly unethical advantages, and 2) it would highlight the value differences between U.S. and Chinese AI and biotechnology firms, which could be an important differentiating factor for firms which handle sensitive personal information like genetic data. These are low-cost ways to partially mitigate some of China's structural advantages in this space.

Recommendation 1.4: Pursue Global Cooperation on Smart Disease Monitoring.

While pivoting to a more competitive national approach toward biotechnology policy, the United States should also pursue efforts to enhance global cooperation on disease monitoring. By pooling existing open-source health-related data with improved early warning signals and data on zoonotic spillovers and transmission of novel viruses, governments will be better postured to use AI to predict and contain future pandemics.[476] The United States should draw from the example of the International Partnership on Avian and Pandemic Influenza, a 2005 initiative announced by President Bush to promote international transparency and data sharing regarding disease outbreaks and pandemics. A reinvigorated push for a new form of this initiative, which would combine increased transparency and data sharing on disease outbreaks with AI tools which have the ability to enhance early outbreak detection and contribute to real-time disease monitoring, could provide substantial benefit for global public health if all countries, including China, participated in good faith.[477]

Such an initiative would require both U.S. and partner support for global disease surveillance capacity building to improve local data collection from potential hotspots, as well as improved integration and standardization of global health-related data, to facilitate the ability of AI to enable improved predictive capabilities. On the former issue, the STOP Spillover program, a $100 million global health security program run by the United States Agency for International Development (USAID) and designed to build capacity in high-risk countries to facilitate early detection of new and dangerous pathogens, is a step in the right direction and could be further expanded in terms of scope.[478] Such efforts should be fully supported by Congress and the Administration moving forward, and mirrored by partner

[476] For additional analysis and opportunities related to global AI cooperation on health-related projects, see Annex B of Tab 5 - Marshal Global AI Cooperation of this report.

[477] For more information on how AI can facilitate improved real-time disease surveillance, see Jason Matheny, et al., *The Role of AI Technology in Pandemic Response and Preparedness: Recommended Investments and Initiatives*, NSCAI at 8-10 (June 25, 2020), https://www.nscai.gov/reports.

[478] The STOP Spillover program is largely a continuation of the PREDICT program, a similar initiative run from 2009-2019 by USAID which identified 931 novel virus species and was widely seen as very successful. See *USAID: Investments in Global Health Security by the U.S. Agency For International Development*, USAID (May 7, 2020), https://www.usaid.gov/news-information/press-releases/may-7-2020-investments-global-health-security-us-agency-international.

nations. Additionally, the United States must support multilateral efforts to collect, aggregate, and standardize relevant zoological data from potential disease hotspots, and combine this data with other regional information on land use, human behavior, and socioeconomic data.

On the latter issue, researchers have already been able to utilize open source health-related data to estimate disease spread even without combining it with relevant zoological data or AI. For instance, hospital traffic extracted from overhead imagery of hospital parking lots has proven to be a useful estimator of disease activity, particularly influenza-like illnesses.[479] Integrating and standardizing such health-related datasets, and combining these two data streams at a global scale, would allow for the utilization of AI technologies to create shared, predictive, global disease monitoring models. An international effort to facilitate disease monitoring using more sophisticated AI models and incorporating predictive on the ground data would simultaneously enhance international security by improving global pandemic defense, while also providing an important model for large-scale global cooperation on AI toward issues of collective benefit.

Part II: Quantum Computing

The Commission is optimistic, but realistic, about the future of quantum computing and its applications to national security. Although classical computers will likely remain the most economical way of performing day-to-day computational tasks in the near future, quantum computers have the potential to outperform their classical counterparts on certain classes of problems related to machine learning and optimization, the simulation of physical systems, and the collection and transfer of sensitive information. Each of these applications create novel national security threats and opportunities at the intersection of artificial intelligence and quantum computing. Although the United States leads its strategic competitors on the research and development of quantum computers, it must be prepared to apply those efforts to national security use cases. In recent years, the United States has jeopardized its access to trusted and assured microelectronics for national security purposes due to its reliance on other nations, including potential adversaries, as a source of semiconductors and their components.[480] Quantum computing represents an opportunity for the United States to reestablish its leadership in the next-generation of computer hardware fueling AI.

To maintain leadership in AI, the United States must take a portfolio approach to investment in next-generation computer hardware. Quantum computers are one of many emerging technologies that offer advantages over traditional CMOS microchip design. For example, purpose-built chips such as graphics processing units (GPUs), application-specific integrated circuits (ASICs), and field-programmable gate arrays (FPGAs) leverage massive parallel processing to train deep neural networks (DNNs) faster than central processing units (CPUs).[481] Similarly, cryogenic computing, silicon photonics, and neuromorphic chips belong to a suite of advanced classical technologies addressed in the Commission's *First*

[479] Elaine O. Nsoesie, *Monitoring Disease Trends Using Hospital Traffic Data from High Resolution Satellite Imagery: A Feasibility Study*, Nature Scientific Reports (Mar. 13, 2015), https://www.nature.com/articles/srep09112.

[480] See e.g., *Interim Report*, NSCAI (Nov. 2019), https://www.nscai.gov/reports; *First Quarter Recommendations*, NSCAI at 45-62 (Mar. 2020), https://www.nscai.gov/reports.

[481] Lynnette Reese, *Comparing Hardware For Artificial Intelligence: FPGAS VS. GPUS VS. ASICS* (July 24, 2018), http://lreese.dotsenkoweb.com/2019/03/30/comparing-hardware-for-artificial-intelligence-fpgas-vs-gpus-vs-asics/.

Quarter Recommendations that promise better performance on certain computational tasks related to AI than existing hardware.[482] However, quantum computers are of particular interest to the Commission because of their potential to generate step-change advantages over today's best supercomputers on tasks directly related to U.S. national security and transform the information environment in which AI is trained and deployed to the battlefield.

To assess the strategic importance of this associated technology, the Commission examines the intersection of quantum computing and AI, identifies the related national security threats and opportunities, and provides a series of recommendations to ensure U.S. leadership in the next-generation of computer hardware.

The Intersection of Quantum Computing and AI

The Commission expressed measured optimism about the future of quantum computing and its impact on AI in the *2019 Interim Report*, noting that the field of quantum machine learning is still in its infancy with few demonstrated improvements over classical models.[483] Yet, the Commission maintains that progress in AI goes hand-in-hand with advances in computing. As the pace of innovation predicted by Moore's Law becomes increasingly difficult for semiconductor manufacturers to maintain due to the physical limits of microchip design (e.g. transistor width, heat dissipation, etc.),[484] leadership in next-generation computer hardware will be essential to preserving U.S. advantages in strategic technologies like AI.

The future of computing will feature a combination of classical and quantum technologies, including cryogenic processors, silicon photonics, and neuromorphic chips. Although the extent of their capabilities remains an open question, quantum computers are at least theoretically capable of solving certain problems in machine learning and optimization faster than their classical counterparts, especially when large amounts of data are required.[485] This asymptotic advantage is derived from the principles of quantum mechanics, which govern the behavior of quantum bits, or "qubits." Qubits are the fundamental units of information in a quantum system and can exist in a complex linear combination, or *superposition*, of two distinguishable states.[486] Put simply, qubits can efficiently perform calculations or simulate quantum systems in ways that classical bits cannot. Qubits can also be *entangled*, a unique property with implications for the future of metrology and communications.

[482] See *First Quarter Recommendations*, NSCAI at 45-62 (Mar. 2020), https://www.nscai.gov/reports.

[483] See *Interim Report*, NSCAI at 51 (Nov. 2019), https://www.nscai.gov/reports.

[484] Steve Blank, *What the GlobalFoundries' Retreat Really Means*, IEEE Spectrum (Sept. 10, 2018). https://spectrum.ieee.org/nanoclast/semiconductors/devices/what-globalfoundries-retreat-really-means.

[485] Although quantum computers do not offer more *computability* than classical computers, they are theoretically capable of solving certain classes of problems in lower *time complexities*. In other words, quantum computers and classical computers can solve the same problems, but quantum computers can theoretically solve a subset of those problems faster than classical computers at scale. See *The Quantum Computing Fact Sheet* (last accessed Sept. 24, 2020), https://quantumfactsheet.github.io/.

[486] The two distinguishable states of such a qubit might be the internal electronic states of an atom, the polarization states of a photon, or the spin states of an atomic nucleus. Therefore, qubits may be physically realized in a number of ways, including superconducting circuits, trapped ions, optical lattices, quantum dots, or linear optics. Quantum computers operate on the state of these qubits using quantum logic gates, which are analogous to classical logic gates except for their physical implementation. For example, if the qubit is realized as an ion, then a quantum logic gate might manipulate the ion's internal energy state with lasers to perform computations. See *Quantum Information Science: An Emerging Field of Interdisciplinary Research and Education in Science and Engineering*, National Science Foundation (Oct. 28-29, 1999), https://www.nsf.gov/pubs/2000/nsf00101/nsf00101.htm#birth.

There are two broad categories of quantum computers: digital and analog. "Digital quantum computers" are general-purpose devices that manipulate the state of qubits to perform computational tasks like a classical computer, but potentially in less time. "Analog quantum simulators" are special-purpose devices used to simulate physical systems that are too complex for classical computers to model efficiently. These devices are theoretically capable of solving problems in applied mathematics (e.g. linear algebra, combinatorial optimization, and graph theory), machine learning (e.g. data-fitting, clustering, and nearest-neighbor classifications), and the simulation of physical systems (e.g. materials science and drug discovery).[487] Many of these applications represent future threats or opportunities with implications for U.S. national security and therefore warrant the Commission's consideration.

National Security Threats and Opportunities Posed by Quantum and AI

Since Peter Shor discovered an algorithm in 1994 that demonstrated quantum computers were capable of factoring integers exponentially faster than classical computers, researchers have made significant strides in the fields of quantum hardware and software.[488] However, fault-tolerant quantum computers (FTQCs) capable of performing general-purpose calculations are still theoretical due to significant technical challenges associated with designing reliable quantum processing units (QPUs).[489] Furthermore, researchers have only been able to demonstrate that quantum algorithms are capable of providing exponential speedups in a handful of applications.[490] It is therefore unlikely that quantum computers will replace the role of classical computers in the near future, if at all. Yet, the United States could still derive advantages in the near-term by investing in noisy intermediate-scale quantum (NISQ) computers that are capable of deriving probabilistic solutions from imperfect qubits.[491] Perhaps the most promising application of NISQ computers lies in a hybrid approach that integrates both quantum and classical components into the same workflow. In particular, the United States should investigate the feasibility of developing QPUs that perform a similar role to that of classical hardware accelerators like GPUs, ASICs, and FPGAs whereby classical computers delegate certain tasks to purpose-built quantum devices designed specifically to help AI systems make faster and more accurate decisions. In the future, if the development of quantum computers follows a trend similar to that of classical computers by which tasks are increasingly performed on the edge rather than

[487] *ASCR Report on Quantum Computing for Science*, U.S. Department of Energy (Oct. 2015), https://www.researchgate.net/publication/282878908_ASCR_Report_on_Quantum_Computing_for_Science.

[488] Peter Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, at 124-134 (1994), https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/12OmNqNXErh/pdf.

[489] If qubits are not adequately isolated from the outside environment, the quantum properties of superposition and entanglement will rapidly decay in a process known as decoherence. In order to forestall decoherence long enough to perform meaningful computations, quantum computers must be kept in supercooled vacuums that are completely isolated from the outside world. Even in this highly controlled environment, error is introduced into the system, potentially invalidating the results of a computation. This noise is combated with an error correction technique that allows researchers to derive high-probability answers to certain computations. See Martin Giles, *Explainer: What is a Quantum Computer?*, MIT Technology Review (Jan. 29, 2019), https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/.

[490] Notable quantum algorithms that demonstrate exponential speedups over their classical counterparts include Shor's algorithm for factoring large numbers, Grover's algorithm for searching through unstructured databases, Lloyd's algorithm for simulating other quantum systems, and the Harrow-Hassidim-Lloyd algorithm for solving linear systems of equations.

[491] Because quantum computers do not currently contain enough qubits to perform error correction properly, researchers have designed noise-resilient quantum algorithms that can be run on NISQ computers. See John Preskill, *Quantum Computing in the NISQ Era and Beyond* (2018), https://arxiv.org/pdf/1801.00862.pdf.

on a server, quantum hardware accelerators have the potential to revolutionize how AI systems make decisions on the battlefield.

Quantum computing will create new national security threats and opportunities by enhancing threats posed by existing AI systems and creating new capabilities which could fundamentally alter the strategic environment. For example, quantum computers may be able to train faster and more precise AI systems in the battlefield, optimize military logistics, or develop new materials for weapons systems. Quantum sensors and communications have the potential to revolutionize the collection and transfer of sensitive information, which directly affects how AI is trained and deployed in national security use cases. Failure to continue investing in the research and development of reliable hardware, open-source software tools, and hybrid quantum-classical algorithms for near-term applications may leave the United States vulnerable to strategic surprise on behalf of competitors. Most notably, China has made significant investments in quantum technologies with military applications in an attempt to offset U.S. strengths.[492]

Due to the strategic implications of quantum computing, the Commission recognizes the importance of establishing trusted sources for critical components of QPUs, ranging from manufacturing equipment to superconducting materials and dilution refrigerators. These components may not yet represent choke points, but as the manufacturing process and materials required to design and produce QPUs continue to advance, these components will inevitably become more specialized. Rather than reshoring the entire supply chain for QPUs, the United States should work with its allies to develop a robust and resilient network of suppliers for critical components that directly impact U.S. national security. Yet, a secure supply chain is not sufficient to ensure that the United States becomes a leader in quantum computing. The United States Government must continue the work it started in the National Quantum Initiative (NQI) Act of 2018 to create a robust research and development ecosystem that attracts top-tier talent and ensures that U.S. national security will benefit from future breakthroughs in the science and technology of quantum computing.[493]

The Commission examined the applications of quantum computing that pose specific national security threats and opportunities in conjunction with AI, as outlined below. These fall into two categories: those with implications for the future of applied math and those that stand to revolutionize the collection and transfer of sensitive information.

Applications to Applied Math

Machine Learning and Optimization

At a fundamental level, quantum computers have the potential to create new risks to U.S. national security risks due to their potential to process information and make decisions more quickly than classical computers in certain scenarios. For example, a sufficiently powerful quantum computer can theoretically perform combinatorial optimization faster than its classical counterpart. AI-enabled systems may use combinatorial optimization in instances where the agent has to satisfy certain criteria given a number of constraints (e.g. planning out a route, scheduling conflicting tasks, or routing a message through a communication

[492] Elsa Kania & John Costello, *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership*, CNAS (2018), https://www.cnas.org/publications/reports/quantum-hegemony.
[493] For more details, see Pub. Law 115-368, National Quantum Initiative Act (2018), https://www.congress.gov/bill/115th-congress/house-bill/6227.

network). These techniques have the potential to impact logistics, electronic warfare, and target selection capabilities. Should quantum computers generate significant performance increases at solving such problems, it could translate into military advantage for the United States or its competitors. Quantum computers may also provide exponential speedups in the fields of linear algebra[494] and machine learning for certain subtasks such as data-fitting, clustering, and nearest-neighbor classifications.[495] Quantum machine learning and optimization remain open fields of research, but the United States must recognize their strategic potential to preemptively mitigate threats and create opportunities related to U.S. national security.

Simulation of Physical Systems

Quantum computers also have potential to efficiently simulate quantum interactions at the atomic scale. Researchers currently use classical AI techniques like deep learning to simulate complex physical systems, but creating a computational model of quantum mechanics is a difficult task for classical computers. Since quantum computers are essentially controllable quantum systems, they can be used to study less controllable quantum systems in fields like condensed-matter physics, high-energy physics, atomic physics, and quantum chemistry.[496] These techniques can be applied to discovering new materials and drugs, modeling climate interactions, or creating precise simulations of complicated weapon systems. Each of these uses could have national security applications. For example, military operations require accurate predictions of climate conditions and military logistics rely on efficient communications networks.[497] Additionally, quantum simulation could aid existing nuclear stockpile stewardship efforts, as quantum computers may be able to produce high fidelity models of the reactions inside a nuclear weapon, facilitating U.S. efforts to maintain confidence in its nuclear arsenal without the use of explosive nuclear testing.[498]

Applications to the Collection and Transfer of Sensitive Information

Sensing

Quantum sensors have the potential to perform more sensitive and precise measurements of physical quantities such as time, acceleration, gravity, and electromagnetic fields by leveraging the quantum behavior of spin qubits, trapped ions, and flux qubits in the form of atomic clocks, accelerometers, gravimeters, and magnetometers.[499] These devices stand to revolutionize how the United States and its strategic competitors carry out intelligence, surveillance, and reconnaissance (ISR) as well as positioning, navigation, and timing

[494] Aram W. Harrow, et al., Quantum algorithm for linear systems of equations (Sept. 30, 2009), https://arxiv.org/pdf/0811.3171.pdf.

[495] *ASCR Report on Quantum Computing for Science*, U.S. Department of Energy (Oct. 2015), https://www.researchgate.net/publication/282878908_ASCR_Report_on_Quantum_Computing_for_Science.

[496] I. M. Georgescu, et al., *Quantum Simulation*, Reviews of Modern Physics (Mar. 10, 2014), https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.86.153; Neil Savage, *Google's Quantum Computer Achieves Chemistry Milestone*, Scientific American (Sept. 4, 2020), https://www.scientificamerican.com/article/googles-quantum-computer-achieves-chemistry-milestone/.

[497] *Advancing Quantum Materials, Efficient Communications Networks*, U.S. Army Research Laboratory (July 24, 2019), https://www.sciencedaily.com/releases/2019/07/190724133703.htm.

[498] *From Bit to Qubits: Pursuing the Quantum Frontier*, Lawrence Livermore National Laboratory: Science & Technology Review (Dec. 2018), https://str.llnl.gov/2018-12/comdec18.

[499] C. L. Degen, et al., *Quantum Sensing*, (June 7, 2017), https://arxiv.org/pdf/1611.02427.pdf.

(PNT).[500] For example, quantum sensors are theoretically more sensitive than classical methods of navigation and timing in environments without reliable access to GPS, including those where GPS is jammed by adversaries.[501] In conjunction with noise reduction techniques enabled by AI, quantum sensors could also collect large quantities of sensitive data with unprecedented precision that could then be transmitted securely via quantum communications networks.[502] AI further amplifies these threats by enabling the rapid processing of collected data pertaining to military operations on a massive scale.

Cryptography and Communications

Quantum computers could be capable of both breaking existing methods of encryption and enabling a new generation of secure communications. Many modern communications channels are protected by an encryption scheme that assumes integer factorization is intractable. In other words, it is believed that conventional computers cannot perform the operations required to decrypt messages in a reasonable amount of time. Public-key cryptography, the most common implementation being RSA, relies on this assumption. However, quantum computers are theoretically capable of factoring large integers efficiently using Shor's algorithm, which would render RSA useless against well-resourced adversaries. The United States and its allies would be forced to redesign everything from their financial systems to their military communications networks in order to prevent strategic competitors from deploying machine learning techniques to derive insight from large volumes of decrypted information, potentially threatening U.S. military personnel or citizens. Although quantum computers capable of breaking RSA are likely far in the future, the potential for strategic surprise is still considerable. Researchers have proposed a number of quantum-resistant encryption schemes, but development remains at a nascent stage, so it would be difficult to quickly deploy these technologies at scale without substantial disruption and cost.[503]

[500] Theresa Hitchens, *AFRL's 'Quantum Collider' Focuses on Boosting ISR, PNT*, Breaking Defense (June 12, 2020), https://breakingdefense.com/2020/06/afrls-quantum-collider-focuses-on-boosting-isr-pnt/.

[501] Charles Q. Choi, *Getting GPS Out of a Jam*, Scientific American (Oct. 1, 2010), https://www.scientificamerican.com/article/getting-gps-out-of-a-jam/.

[502] Interagency Working Group on Quantum Information Science of the Subcommittee on Physical Sciences, *Advancing Quantum Information Science: National Challenges and Opportunitie*s, The White House (July 2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Quantum_Info_Sci_Report_2016_07_22%20final.pdf.

[503] Although research suggests a quantum computer capable of executing Shor's algorithm is still far off, researchers have already developed initial techniques for communication that are robust to adversaries with advanced quantum capabilities. These communication networks are systems that transmit qubits, typically in the form of photons, via optical cables. Because the qubits are in a state of superposition, a middle-man who attempts to observe the network traffic destroys the qubit's quantum state, allowing the intended recipient to detect the malicious activity. Quantum key distribution (QKD) leverages this convenient phenomenon so that two parties can share cryptographic keys without having to worry about a "man-in-the-middle" (MITM) attack. Because QKD is difficult to implement in practice, researchers have also proposed using quantum teleportation to transmit information securely. However, both of these new technologies are unlikely to replace networking via the current internet given the vast quantities of information and the difficulty of maintaining qubits' state of superposition during transmission. See Martin Giles, *Explainer: What is Quantum Communication?*, MIT Technology Review (Feb. 14, 2019), https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/.

U.S. and Competitor Postures on AI and Quantum Sciences

United States. The U.S. public and private sectors have invested substantially in quantum computing and much of the cutting-edge research in the field is performed in the United States as a result.[504] The bipartisan National Quantum Initiative (NQI) Act of 2018 took a series of steps that establish quantum information science (QIS) as a strategic priority for the United States. As part of this push, the Department of Energy (DoE) recently announced $625 million to establish five QIS research centers over five years led by the national laboratories.[505] The National Science Foundation (NSF) announced $75 million to create three Quantum Leap Challenge Institutes over the same period.[506] Lastly, the President's FY 2021 Budget recommended doubling federal investment levels in quantum technologies by 2022.[507] This continuing investment is necessary to determine the full potential of quantum computing and maintain the United States' position of leadership in next-generation computer hardware.

The United States Government has done well to invest in the fundamental science of quantum computing, but it must also fully recognize the future threats and opportunities that quantum computing poses to national security. To this end, DARPA is actively involved in the research and development of noise-resistant quantum hardware and algorithms through its Optimization with Noisy Intermediate-Scale Quantum (ONISQ) program.[508] Because China's strategy of military-civil fusion allows it to rapidly develop military use cases for dual-use technologies like quantum computing and AI, the United States risks falling behind if it does not work closely with industry to create a robust commercial quantum computing ecosystem and domestic supply chain. The Quantum Economic Development Consortium (QED-C) is a promising effort to achieve this goal led by the National Institute of Standards and Technology (NIST).[509] The United States must take advantage of cutting-edge research performed by U.S. academia and industry to generate strategic advantage on the battlefield.

China. China seeks to lead the "second quantum revolution" and has announced billions of dollars of investment to this end through a series of megaprojects and national laboratories focused on quantum technologies.[510] According to the "Science, Technology, and Innovation 2030 Plan," leadership in quantum communications is a particular priority for China.[511] In fact, China was the first to launch a quantum communications satellite known

[504] Elizabeth Gibney, *Quantum Gold Rush*, *Nature* (Oct. 2, 2019). https://www.nature.com/articles/d41586-019-02935-4.

[505] *Department of Energy Announces $625 Million for New Quantum Centers*, U.S. Department of Energy (Jan. 10, 2020), https://www.energy.gov/articles/department-energy-announces-625-million-new-quantum-centers.

[506] *NSF Establishes 3 New Institutes to Address Critical Challenges in Quantum Information Science*, National Science Foundation (July 21, 2020), https://www.nsf.gov/news/special_reports/announcements/072120.jsp.

[507] *Recommendations for Strengthening American Leadership in Industries of the Future,* The President's Council of Advisors on Science and Technology at 5 (2020), https://science.osti.gov/-/media/_/pdf/about/pcast/202006/PCAST_June_2020_Report.pdf?la=en&hash=019A4F17C79FDEE5005C51D3D6CAC81FB31E3ABC.

[508] Tatjana Curcic, *Optimization with Noisy Intermediate-Scale Quantum Devices*, DARPA (last accessed Sept. 25, 2020), https://www.darpa.mil/program/optimization-with-noisy-intermediate-scale-quantum-devices.

[509] *Who We Are*, The Quantum Consortium (last accessed Sept. 25, 2020), https://quantumconsortium.org/.

[510] Elsa B. Kania, *China's Quantum Future*, Foreign Affairs (Sept. 27, 2018), https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future.

[511] Michael Brown & Pavneet Singh, Brown, *China's Technology Transfer Strategy,* Defense Innovation Unit Experimental (Jan. 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

as Micius in 2016, which it developed indigenously.[512] That same year, China completed the world's longest terrestrial quantum communications network that extends 2,000 kilometers from Beijing to Shanghai. These developments may be driven by the PLA belief that quantum technologies could serve as a potential "offset" to U.S. military power.[513]

Although China lags behind the United States in the fundamental research and development of quantum computers, its extensive investment in quantum applications, particularly those with national security implications, could give it an advantage in strategic use cases. In 2018, China had almost twice as many patent filings as the United States for quantum technology overall, including quantum communications and cryptography, even though the United States leads in quantum computer patents.[514] If this gap between the United States and China in quantum applications persists, it could pose significant national security threats when quantum technology becomes sufficiently advanced.

Russia. Russian efforts in quantum computers most likely trail those in the United States and China.[515] The country's first working prototype of a quantum computer featured two qubits and was launched in 2019.[516] That December, Russia announced a $790 million quantum initiative to be carried out over five years according to the "Russian Quantum Technologies Roadmap." However, these initiatives lack the focus on national security applications that China stresses. Russia has not stated publicly how it might apply these developments to its military.[517]

Recommendation 2.1: Publicly Announce Government Interest in Specific Quantum Use Cases to Incentivize Transition from Basic Research to National Security Applications.

As the world leader in many areas of quantum computing research and development, the United States is well-positioned to take advantage of its early success. However, to realize the practical applications of quantum technologies, the United States must increase its focus on transitioning its efforts in basic science to national security applications that have the potential to revolutionize how the U.S. military operates. In order to expedite this transition for quantum computing, the United States Government should consider publicly announcing a set of specific use cases for quantum computers that it is interested in pursuing. By reflecting the combined views of entities engaging with the private sector, this would signal that a market for practical applications of quantum computers exists, set forth specific goals for those applications, and incentivize additional commercial investment. Some applications of quantum computing will be too sensitive to reveal publicly, but announcing a

[512] *Emerging Military Technologies: Background and Issues for Congress,* Congressional Research Service at 23 (Aug. 4, 2020). https://fas.org/sgp/crs/natsec/R46458.pdf.

[513] Elsa Kania & John Costello, *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership*, CNAS (2018), https://www.cnas.org/publications/reports/quantum-hegemony.

[514] Jeanne Whalen, *The Quantum Revolution is Coming, and Chinese Scientists Are at the Forefront*, Washington Post (Aug.18, 2019), https://www.washingtonpost.com/business/2019/08/18/quantum-revolution-is-coming-chinese-scientists-are-forefront/.

[515] Quirin Schiermeier, *Russia Joins Race to Make Quantum Dreams a Reality*, Nature (Dec. 17, 2019), https://www.nature.com/articles/d41586-019-03855-z.

[516] James Dargan, *Is Russia's Absence from the Quantum Computing Tech Space About to End?*, The Quantum Daily (Dec. 17, 2019), https://thequantumdaily.com/2019/12/17/is-russias-absence-in-qc-tech-space-about-to-end/.

[517] *Emerging Military Technologies: Background and Issues for Congress,* Congressional Research Service at 23 (Aug. 4, 2020). https://fas.org/sgp/crs/natsec/R46458.pdf.

subset of applications of interest openly will provide important direction and energy to U.S. industry.

The Department of Defense (DoD) is still refining its organization-wide approach to rapidly transition commercial technologies from research to fielding in high-cost, hardware-intensive sectors with long development horizons such as quantum computing. In the long-term, it should prioritize efforts to establish an integrated approach to rapid technology procurement across its innovation offices, which could take several years of dedicated effort to rationalize and specialize each organization's role. In the interim, public announcements of priority applications will help spur private sector investment and innovation in transitioning quantum technologies despite the absence of an integrated technology procurement apparatus.

Recommendation 2.2: Make Quantum Computing Accessible to Researchers via the National AI Research Resource.

The United States has an opportunity to cement its leadership on quantum computing by providing access to both classical and quantum computers via the National AI Research Resource, which the Commission recommended establishing in its *First Quarter Recommendations*.[518] Doing so would help industry, academia, and government researchers to build and test software tools and algorithms that leverage both classical and quantum computers in a hybrid fashion. Currently, there is no single resource provided by the United States Government that seamlessly integrates both classical and quantum computers into the same workflow.[519] Such a resource would encourage the development of hybrid quantum-classical algorithms for machine learning in the near-term, lower barriers to innovation for small start-ups in the quantum computing space, and attract talent from around the globe. This type of resource may also facilitate public-private partnerships that encourage commercialization of quantum technologies and help the United States Government adopt those products for military use cases.

Recommendation 2.3: Foster a Vibrant Domestic Quantum Fabrication Ecosystem.

Because quantum computing could exponentially increase the power of AI, the United States must take steps now to cement its long-term status as the global leader in the design and manufacturing of quantum processing units (QPUs). Although superconducting materials and dilution refrigerators do not currently represent a choke point in the supply chain for quantum computers, the United States Government must play a leading role in cultivating domestic fabrication capabilities to prevent a recurrence of the circumstances it currently finds itself in with respect to semiconductor fabrication. For example, because superconductors will likely be key to the next generation of both quantum and classical computers, the United States must recognize the strategic importance of fabricating these

[518] See *First Quarter Recommendations*, NSCAI at 12-13 (Mar. 2020), https://www.nscai.gov/reports.

[519] The Department of Energy and the Air Force do offer access to commercial quantum capabilities but this access is not government-wide, nor is it focused on hybrid quantum-classical applications to national security. See *Air Force Research Laboratory to Join IBM Q Network as First DOD-led IBM Q Hub*, Wright-Patterson AFB (Aug. 2, 2019), https://www.wpafb.af.mil/News/Article-Display/Article/1924271/air-force-research-laboratory-to-join-ibm-q-network-as-first-dod-led-ibm-q-hub/; Adrian Cho, *After Years of Avoidance, Department of Energy Joins Quest to Develop Quantum Computers*, Science (Jan. 10, 2018), https://www.sciencemag.org/news/2018/01/after-years-avoidance-department-energy-joins-quest-develop-quantum-computers.

components domestically. The same logic applies to other advanced materials in the supply chain for quantum devices. If the United States Government offers adequate incentives for the research and development of quantum computers and their components while simultaneously creating demand for national security applications of quantum technologies, the United States could extend its leadership in next-generation computer hardware for years to come. The recently established Quantum Economic Development Consortium (QED-C), first proposed in the National Quantum Initiative (NQI) Act of 2018, is an important step in this direction.

Congress should enact a package of provisions that incentivizes the domestic design and manufacturing of quantum computers and their constituent materials. A tax credit for expenditures made in the United States on research and development, manufacturing equipment, and workforce training related to the development of quantum technologies is a necessary, albeit not sufficient, step to maintain U.S. competitiveness in this area. This provision could be modeled on the Alternative Simplified Credit (ASC), which provides a credit of fourteen percent of expenditures on research and development in excess of fifty percent of base period expenditures, or as an extension of the microelectronics tax credit proposed in Recommendation 3.1 to cover any quantum components not already included. However, it is important to note that while tax credits are beneficial for large corporations investing in quantum computers, they may be less useful to startups on the cutting edge of research and development that are not yet profitable. Because of the high upfront costs associated with building quantum computers, these firms need access to funding that will help them scale, potentially in the form of a loan guarantee from the United States Government or equity financing. See Recommendation 3.4 for more details on how the United States Government could deploy a broad array of financial instruments to incentivize the domestic production of emerging technologies.

Part III: Microelectronics Leadership and Critical Technology Supply Chain Resilience

In its *2019 Interim Report* and quarterly recommendations to date, the Commission has identified U.S. leadership in microelectronics as essential to overall U.S. leadership in AI. The Commission has also concluded that the U.S. retains strategic advantages in microelectronics, but its leadership is eroding, especially in the manufacturing, assembly, packaging and testing of semiconductors. In those areas of the electronics value chain, the U.S. is overly dependent upon globally diversified supply lines, including imports from potential adversaries. As a result of these gaps in the U.S. industrial base, the risks are increasing that the United States could lose access to trusted, assured, and state-of-the-art semiconductors for national security purposes.

Building on its *2019 Interim Report*, the Commission submitted *First Quarter Recommendations* focused on actions to promote U.S. leadership in microelectronics.[520] Recommendations included supporting long-term access to resilient, trusted, and assured microelectronics for AI and taking a portfolio-based approach to running faster than potential adversaries in the field of cutting-edge microelectronics. In April, three commissioners and select Commission staff offered targeted recommendations as part of a temporary special project on the AI-related aspects of pandemic response for mitigating the impact of COVID-19 on AI-enabling

[520] *First Quarter Recommendations*, NSCAI at 45-62 (Mar. 2020), https://www.nscai.gov/reports.

technology supply chains and increasing U.S. competitiveness.[521] Finally, the Commission released tailored recommendations in Q2 on protecting U.S. national security advantages in hardware through targeted export controls, while recognizing that controls cannot supplant investment and innovation.[522]

The Commission has been encouraged by a number of developments over the past several months related to U.S. microelectronics leadership. Highlights include newly announced efforts to revitalize domestic fabrication of state-of-the-art microelectronics, such as Taiwan Semiconductor Manufacturing Company's (TSMC) decision to develop an advanced facility in the United States, Intel's public interest in working with the United States government to develop a commercial U.S. foundry, and the inclusion of key elements of the "CHIPS for America Act" in the House and Senate versions of the FY 2021 NDAA. However, microelectronics and their supply chains represent only one of several industrial sectors critical to U.S. leadership in AI and associated technologies.[523]

Therefore, while promising, these recent actions represent only the initial steps needed to prepare for sustained technological competition with China. More remains to be done to continue leading in microelectronics, to secure critical supply chains in other emerging technologies, and to generate enduring national technology leadership. Building on previous work in these areas, the following section offers recommendations to further promote AI-enabling microelectronics domestically and improve the resilience of U.S. supply chains for the full suite of critical technologies.

Issue 1: Developing a Resilient Domestic Microelectronics Industrial Base

Passing key elements of the CHIPS for America Act in the FY 2021 NDAA would have a substantial and enduring impact on U.S. microelectronics leadership. This is critical now more than ever, especially since not all recent news regarding U.S. semiconductor manufacturing has been positive. In July, Intel revealed that it has encountered challenges in the development of its manufacturing process for 7nm semiconductors, likely delaying its original target for delivering 7nm chips from 2021 to at least 2022.[524] To overcome this challenge, Intel is considering outsourcing manufacturing to a commercial foundry for the first time in the firm's history.[525] As the last remaining U.S. firm striving to maintain a leading-edge manufacturing capability, Intel potentially exiting the state-of-the-art manufacturing market and outsourcing fabrication to a foreign firm represents a substantial threat to U.S. leadership in microelectronics. If Intel outsources manufacturing to a firm in another nation such as Taiwan or South Korea, the United States must also contend with the second-order, systemic challenges of retaining the deep technical expertise, tacit knowledge, and professional networks needed to develop state-of-the-art chip fabrication

[521] Chris Darby, et al., *Mitigating Economic Impacts of the COVID-19 Pandemic and Preserving U.S. Strategic Competitiveness in Artificial Intelligence*, NSCAI (May 19, 2020), https://www.nscai.gov/reports.

[522] *Second Quarter Recommendations*, NSCAI at 48-77 (July 2020), https://www.nscai.gov/reports.

[523] See Michael Brown, et al., P*reparing the United States for the Superpower Marathon with China*, Brookings (Apr. 2020), https://www.brookings.edu/research/preparing-the-united-states-for-the-superpower-marathon-with-china/.

[524] *Intel Reports Second-Quarter 2020 Financial Results*, Intel (July 23, 2020), https://www.intc.com/news-events/press-releases/detail/1402/intel-reports-second-quarter-2020-financial-results.

[525] Ian King, *Intel Plunges as It Weighs Exit From Manufacturing Chips*, Bloomberg (July 24, 2020), https://www.bloomberg.com/news/articles/2020-07-24/intel-considers-what-was-once-heresy-not-manufacturing-chips.

domestically.[526] Challenges around government incentives and the availability of highly-skilled employees apply equally to Intel's outsourcing decision and TSMC plans for constructing a fabrication facility in Arizona.[527] If the underlying networks of expertise degrade it will be even harder to build them back to serve domestic firms such as Intel or convince foreign firms such as TSMC to locate facilities in the United States.

Intel may be forced to outsource to firms in Taiwan or South Korea in part because those nations have publicly invested in and incentivized the infrastructure and human capital required to sustain their semiconductor industries over the long term. A recent study estimated that the 10-year total cost of ownership of a fabrication facility in the United States is 30 percent greater than in Taiwan, Singapore, and South Korea.[528] Moreover, between 40 and 70 percent of that cost differential is directly attributable to government incentives.[529] Drawing on these government incentives and networks of semiconductor manufacturing expertise, TSMC in Taiwan and Samsung in South Korea are likely better positioned to bounce back if they face a process slip similar to Intel's recent misstep. In contrast, the United States' eroding semiconductor manufacturing base has drained the nation's stock of specialized engineering talent and the enabling R&D networks in academia and government required for chip production. Therefore, onshoring manufacturing of leading edge and specialized chips in the United States will require more than tax breaks and public spending on R&D. Successful reshoring must build the larger support system needed to create a competitive market of small and medium sized firms, a resilient supply chain, and a world class workforce. It will also require building the domestic talent pool for microelectronics, a focus area of the recommendations in Tab 3 of this report on microelectronics scholarships and curriculum development.[530] Rebuilding and sustaining a resilient microelectronics industrial base will take time and the application of a broad range of policy tools across research, talent, manufacturing, and more.

Recommendation 3.1: Incentivize Domestic Leading-Edge Microelectronics by Authorizing and Fully Funding Key Provisions of the CHIPS for America Act, including the Advanced Packaging National Manufacturing Institute

To incentivize the development by the private sector of a state-of-the-art domestic commercial foundry, NSCAI strongly supports the provisions from the CHIPS for America Act (H.R.7178 / S.3933) included in the Senate and House versions of the NDAA via

[526] Rush Doshi, *The United States, China, and the Contest for the Fourth Industrial Revolution*, Brookings (July 31, 2020), https://www.brookings.edu/testimonies/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution/.

[527] TSMC Announces Intention to Build and Operate an Advanced Semiconductor Fab in the United States, TSMC (May 15, 2020), https://www.tsmc.com/tsmcdotcom/PRListingNewsArchivesAction.do?action=detail&newsid=THGOANPGTH&language=E.

[528] Antonio Varas, *Government Incentives and US Competitiveness in Semiconductor Manufacturing*, Boston Consulting Group & Semiconductor Industry Association at 1 (Sept. 2020), https://www.semiconductors.org/wp-content/uploads/2020/09/Government-Incentives-and-US-Competitiveness-in-Semiconductor-Manufacturing-Sep-2020.pdf.

[529] Id.

[530] See Tab 3 Recommendations for proposed microelectronics workforce actions.

amendments.[531] Both amendments contain overlapping and unique provisions from the CHIPS for America Act to strengthen the U.S. microelectronics manufacturing and research base. This package of legislative proposals would also provide significant increases in funding for several programs the Commission has previously identified as essential to U.S. microelectronics leadership. In particular, key provisions would boost semiconductor research funding and development of advanced packaging and interconnect technologies. It would also establish national centers of excellence for microelectronics and an incubator for semiconductor startup firms, mirroring a previous Commission recommendation to study the viability of a national microelectronics laboratory and incubator.[532] However, even if these provisions become law in the NDAA, they must still receive appropriated funding to have an impact. Authorizing and fully funding these provisions are critical steps for developing and sustaining a leading-edge commercial fabrication capability for microelectronics in the United States.

Proposed Legislative Branch Action

Include key elements of the CHIPS for America Act from the House and Senate NDAAs in the FY 2021 NDAA and fully fund these programs through the FY 2021 appropriations process.

Recommendation 3.2: Create Private Sector Incentives for Developing a Leading-Edge Merchant Fabrication Facility Through Refundable Investment Tax Credits

The CHIPS for America Act provisions included in the House and Senate versions of the NDAA do not include the 40 percent refundable federal investment tax credit (ITC) for semiconductor manufacturing facilities and equipment. This incentive would reduce a semiconductor firm's tax bill by 40 percent on semiconductor manufacturing equipment and facilities through 2024, followed by reduced tax credit rates of 30 percent and 20 percent, respectively, in 2025 and 2026.[533] Existing U.S. incentives reduce the cost of foundry construction attributable to capital expenses, operating expenses, and taxes by roughly 10 to 15 percent. In South Korea, Taiwan, and Singapore, the incentives are roughly twice that of the United States, resulting in an estimated 25 to 30 percent cost reduction.[534] This gap is one driving factor behind the lack of an advanced logic merchant foundry in the United States.[535] Closing this gap will incentivize U.S. firms to construct facilities domestically while also attracting foreign firms such as TSMC.

[531] Provisions of H.R.7178 and S.3933 were incorporated in the Senate and House NDAAs during the amendment process. See S. 4049, National Defense Authorization Act for Fiscal Year 2021, Amdt. 2244, https://www.congress.gov/congressional-record/2020/06/29/senate-section/article/S3658-1 and H.R. 6395, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Amdt. 597, https://amendments-rules.house.gov/amendments/MATSUI_070_xml71720090438438.pdf.

[532] *First Quarter Recommendations*, NSCAI at 53 (Mar. 2020), https://www.nscai.gov/reports.

[533] *Bipartisan, Bicameral Bill Will Help Bring Production of Semiconductors, Critical to National Security, Back to U.S.*, John Cornyn (June 10, 2020), https://www.cornyn.senate.gov/node/5599#:~:text=McCaul.,and%20phases%20out%20in%202027.

[534] Antonio Varas, *Government Incentives and US Competitiveness in Semiconductor Manufacturing*, Boston Consulting Group & Semiconductor Industry Association (Sept. 2020), https://www.semiconductors.org/wp-content/uploads/2020/09/Government-Incentives-and-US-Competitiveness-in-Semiconductor-Manufacturing-Sep-2020.pdf

[535] Id.

To strengthen the U.S. economy, enhance national security, and promote supply chain resilience, the United States needs to compete with other countries in attracting the construction and operation of new fabs by establishing grant and tax incentives, especially for leading edge firms. The Commission also previously highlighted the importance of tax credits along these lines in its *Second Quarter Recommendations*.[536] While included in the draft HEALS Act, it remains to be seen whether this key provision will be included in the final version of any pending legislation. Ensuring this provision becomes law will reward investment, make the United States a more attractive destination for constructing cutting-edge fabrication facilities, and support U.S. industries efforts to compete in the global semiconductor market.[537]

Proposed Legislative Branch Action

Pass legislation adopting the CHIPS for America Act semiconductor investment tax credit for 40 percent on semiconductor manufacturing equipment and facilities through 2024, followed by reduced tax credit rates of 30 percent and 20 percent, respectively, in 2025 and 2026.

Issue 2: Promoting Resilient Supply Chains for Critical Technologies

Maintaining secure and resilient U.S. supply chains is a challenge as old as the nation. As early as 1790, President George Washington shared his view with Congress that "[a free people's] safety and interest require that they should promote such manufactories, as tend to render them independent on others, for essential, particularly for military supplies."[538] To address the threat at that time of relying on military imports from potentially hostile Britain and France, the United States Government used public funding in 1794 to establish national arsenals, which helped spawn an innovative U.S. weapons industry in the 19th century.[539]

While the complexity of military equipment and its supply chains have increased exponentially since the nation's founding, the basic problem remains the same. Today the development and manufacture of high-tech goods for AI and associated technologies are as important to national security as muskets, cannons, and ammunition in the 18th century. Yet, over the last decade, the total number of suppliers based in China in the Department of Defense's supplier base increased by 420 percent, to a total of 655 firms.[540] Over the same period, the proportion of suppliers based in China within DoD supply lines specifically for critical industries grew from six percent to nine percent compared to the U.S. and other nations.[541] In recent months, COVID-19 has further highlighted the strategic importance of supply chains as an element of geoeconomic competition. Recognizing this, President Xi Jinping explicitly stated that protecting China's supply chains is one of China's top six

[536] *Second Quarter Recommendations*, NSCAI (July 2020), https://www.nscai.gov/reports.

[537] Rob Atkinson, *On Tax Incentives*, American Compass (June 8, 2020), https://americancompass.org/essays/on-tax-incentives/.

[538] *From George Washington to the United States Senate and House of Representatives*, National Archives (Jan. 8, 1790), https://founders.archives.gov/documents/Washington/05-04-02-0361.

[539] Tom Cotton, *Foreword: On Security*, American Compass (May 4, 2020), https://americancompass.org/essays/tom-cotton-foreword-on-security/; Daniel Else, *The Arsenal Act: Context and Legislative History*, Congressional Research Service (Oct. 28, 2011), https://fas.org/sgp/crs/natsec/R42062.pdf.

[540] *The Challenge Of Reshoring The Defense Department Supply Chain*, Govini (2020), https://www.govini.com/wp-content/uploads/2020/08/Govini-DoD-Reshoring-Challenge.pdf.

[541] Id.

national priorities for recovering from COVID-19.[542] China has also shown the world it is willing to use its control of certain goods to influence other countries, including the U.S. and its allies. If the United States cannot anticipate these commercial dependencies, it will struggle to respond or help allies respond to China's actions.[543]

The Commission's analysis and recommendations to date have focused on the resiliency of the U.S. microelectronics supply chain, highlighting vulnerabilities and proposing actions to improve access to secure, trusted, and state-of-the-art semiconductors. However, microelectronics is just one of several industrial sectors critical to national security. Studies by DoD have also identified risks in the supply chains for rare earth minerals, active pharmaceutical ingredients, and other materials.[544] Recognizing that supply chains for emerging technology are highly globalized, the actions the United States Government should take to promote reshoring in this area are also applicable for improving domestic access to other critical sectors as well. To address these challenges, the following recommendations would first improve the United States Government's capacity to analyze supply chain risks and second take coordinated action to incentivize the reshoring of critical industries, especially for AI and associated technologies.

Recommendation 3.3: Improve Supply Chain Analysis, Reporting, and Stress Testing

As select Commissioners and staff recommended in the Commission's *Mitigating Economic Impacts of the COVID-19 Pandemic and Preserving U.S. Strategic Competitiveness in Artificial Intelligence*, securing supply chains first requires identifying gaps and prioritizing across industries.[545] This analysis should focus on developing categories of goods that are critical and must be produced domestically; goods that can safely be sourced from allies and partners; and goods that can continue to be imported from the global market, including from China.

Mitigating Economic Impacts of the COVID-19 Pandemic and Preserving U.S. Strategic Competitiveness in Artificial Intelligence specifically recommended that Congress establish a unit within the National Institute of Standards and Technology charged with understanding U.S. capabilities and gaps in domestic advanced technology production.[546] Building on that recommendation, the President should direct the agencies responsible for producing economic statistics—specifically the Census Bureau, the Bureau of Economic Analysis, and the U.S. International Trade Commission—to update their methodologies for collecting and publishing detailed supply chain data on critical industries to provide deeper insights into the

[542] Rush Doshi, *The United States, China, and the Contest for the Fourth Industrial Revolution*, Brookings (July 31, 2020), https://www.brookings.edu/testimonies/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution/.
[543] Id.
[544] *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, U.S. Department of Defense (Sept. 2018), https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.
[545] Chris Darby, et al., *Mitigating Economic Impacts of the COVID-19 Pandemic and Preserving U.S. Strategic Competitiveness in Artificial Intelligence*, NSCAI (May 19, 2020), https://www.nscai.gov/reports.
[546] Id. at 17.

country of origin of the components of imported goods.[547] Additionally, the Census Bureau should also be required to resume its past practice of preparing annual "Current Industrial Reports" at the ten-digit industry level for AI and associated industries, since this information will be critical for developing effective reshoring and resilience policies.[548]

Most importantly**,** the United States Government should work with industry to design and execute supply chain stress testing for companies in critical industries for national security, starting with microelectronics. As COVID-19 has demonstrated, the rise of just-in-time manufacturing and lean production has reduced the resilience of supply chains when facing natural disasters, foreign interference, or other disruptions. Similar to the stress tests required by Dodd-Frank for financial institutions after the 2008 financial crisis, supply chain stress tests would help determine two key data points for strategically critical goods: time to recover and time to survive.[549] Time to recover is the length of time required for a node in the supply chain (e.g., a supplier facility, a distribution center, or a transportation hub) to be restored to full functionality after a disruption. Time to survive is the maximum duration that the supply chain can match supply with demand after a facility disruption. By quantifying each measure under different scenarios and creating a standard methodology for industry to adopt, the United States Government can begin to assess its resilience and prioritize its reshoring strategy accordingly.[550] The microelectronics industry would be the first industry to assess. Just as stress testing has improved insight into the resilience of U.S. financial institutions, supply chain stress tests could enhance existing supply chain risk management practices and drive improvements in resilience in the private sector among firms supplying critical technology for national security purposes.[551]

Proposed Executive Branch Action

Establish a unit within the National Institute of Standards and Technology charged with understanding U.S. capabilities and gaps in domestic advanced technology production. The President should direct the Census Bureau, the Bureau of Economic Analysis, and the U.S. International Trade Commission to update their methodologies for import component analysis. Direct the Census Bureau to resume preparing annual "Current Industrial Reports" for AI and associated technologies. Direct the development and execution of a standardized supply chain stress test for systemically important firms producing critical technologies for national security, starting with microelectronics.

[547] This mirrors recommendations made in 2019 by the U.S. China Economic Secretary Review Commission. See *2019 Report To Congress*, U.S.-China Economic And Security Review Commission at 537-545 (Nov. 2019), https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf.

[548] See also *2019 Report To Congress*, U.S.-China Economic And Security Review Commission at 537-545 (Nov. 2019), https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf; Rush Doshi, *The United States, China, and the Contest for the Fourth Industrial Revolution*, Brookings (July 31, 2020), https://www.brookings.edu/testimonies/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution/.

[549] Id.

[550] David Simchi-Levi & Edith Simchi-Levi, *We Need a Stress Test for Critical Supply Chains*, Harvard Business Review (Apr. 28, 2020), https://hbr-org.cdn.ampproject.org/c/s/hbr.org/amp/2020/04/we-need-a-stress-test-for-critical-supply-chains.

[551] *Federal Reserve Board Releases Results of Stress Tests for 2020 and Additional Sensitivity Analyses Conducted in Light of the Coronavirus Event*, Board of Governors of the Federal Reserve System (June 25, 2020), https://www.federalreserve.gov/newsevents/pressreleases/bcreg20200625c.htm.

Recommendation 3.4: Centralize Reshoring and Supply Chain Management

While simultaneously improving the capacity to analyze supply chain risks, the United States Government must also prepare the organizations and policy tools necessary to successfully restore and diversify the supply chains of industries it identifies as critical. This will take commitment and substantial resources given that U.S. companies have spent massively to expand their offshore supply chains, with estimates of overseas direct investments for production by U.S. firms ranging up to $6 trillion.[552]

To respond to the supply chain disruptions caused by COVID-19, the White House created a Supply Chain Stabilization Task Force focused on the critical medical supplies needed to respond to the pandemic.[553] In addition, the White House repurposed and expanded the mission of the recently established U.S. International Development Finance Corporation (DFC) through Executive Order in May.[554] Previously known as the Overseas Private Investment Corporation, it became the DFC in December 2019, gaining new missions and authorities for financing projects in developing nations along with its new name. In the wake of COVID-19, however, it has been tasked with providing domestic loans for U.S. supply chain reshoring under the authority of the Defense Production Act. This new mission is outside DFC's core mandate of financing for developing countries and it has required rapidly hiring 15 people (out of a staff of 337) to focus on it.[555] While this speed and adaptation is necessary and inspiring, it is also emblematic of a broader problem. Policymakers are hampered in the development of wide supply-chain strategy and policy by the near-term issues surrounding the medical supply chain and the diffusion of responsibilities and authorities across a hodgepodge of agencies. The DFC's mandate, structure, and expertise are not suited to focus on domestic reshoring over the long-term without systemic changes to the organization.

The United States Government should draw on the lessons of its allies and partners in designing its approach to reshoring. Taiwan, for example, has successfully applied a wide range of policy instruments beyond tax credits and subsidies to reshore $33 billion worth of

[552] Jacob Helberg, *In the New Cold War, Deindustrialization Means Disarmament*, Foreign Policy (Aug. 12, 2020), https://foreignpolicy.com/2020/08/12/china-industry-manufacturing-cold-war/; Riley Walters, *It's Naive to Assume "Supply Chains" Will Return to the U.S.*, The Heritage Foundation (Apr. 27, 2020), https://www.heritage.org/trade/commentary/its-naive-assume-supply-chains-will-return-the-us.

[553] Statement of Rear Admiral John Polowczyk, Department Of Defense: Supply Chain Stabilization Task Force, before The Select Subcommittee On The Coronavirus Crisis United States House Of Representatives (July 2, 2020), https://docs.house.gov/meetings/VC/VC00/20200702/110851/HHRG-116-VC00-Wstate-PolowczykR-20200702.pdf

[554] Donald J. Trump, *Executive Order on Delegating Authority Under the DPA to the CEO of the U.S. International Development Finance Corporation to Respond to the COVID-19 Outbreak*, The White House (May 14, 2020), https://www.whitehouse.gov/presidential-actions/eo-delegating-authority-dpa-ceo-u-s-international-development-finance-corporation-respond-covid-19-outbreak/.

[555] David Lawder, *Exclusive: New U.S. Development Agency Could Loan Billions for Reshoring, Official Says*, Reuters (June 23, 2020), https://www.reuters.com/article/us-usa-trade-reshoring-exclusive/exclusive-u-s-development-agency-could-loan-billions-for-reshoring-official-says-idUSKBN23U31F; David Vergun, *DOD Partners With DFC to Protect Industrial Base From Economic Effect of Pandemic*, U.S. Department of Defense (June 22, 2020), https://www.defense.gov/Explore/News/Article/Article/2227560/dod-partners-with-dfc-to-protect-industrial-base-from-economic-effect-of-pandem/; *DFC to Sign Letter of Interest for Investment in Kodak's Expansion Into Pharmaceuticals*, U.S. International Development Finance Corporation (July 28, 2020), https://www.dfc.gov/media/press-releases/dfc-sign-letter-interest-investment-kodaks-expansion-pharmaceuticals.

economic activity since 2019.[556] Taiwan's approach includes offering a broad package of incentives such as rent assistance, cheap finance, land acquisition, and simplified reinvestment provisions. However, the key to Taiwan's success has been creating a "a one-stop shop to help manufacturers return home smoothly," designated as "Invest Taiwan," in the Ministry of Economic Affairs.[557] Taiwan's results show the importance of designating one office to serve as a single point of contact for all firms considering leaving China and then empowering that office to work with businesses to tackle the challenges they face.[558]

As a first step, the Federal Government should bring together representatives from the Departments of State, Defense, and Commerce, the U.S. Trade Representative, the Small Business Administration, export promotion agencies, and others as needed into a fusion cell for reshoring and resilience.[559] The mission of this fusion cell would be broader than the existing supply chain stabilization task force. This team would oversee all U.S. supply chain reshoring efforts and serve as a single interface for firms considering diversifying their supply chains to the U.S. or allied nations. By fusing existing resources and authorities rather than standing up an entirely new bureau, office, or agency (as others have proposed) this cross functional team would concentrate the government's focus and provide a single point of contact for industry without substantially increasing overhead. Moving beyond existing reshoring efforts related to the medical supply chain, it should focus attention on microelectronics first and then a broader list of emerging technologies identified through the analyses recommended in Recommendation 3.3.

Over the long term, the United States should sharpen its tools for financing reshoring initiatives through loans, non-dilutive capital, and other incentives. The Defense Production Act offers wide latitude for making loans in this area, but no organization currently has the authority to combine loans with a broader range of financial incentives to bring home the key elements of critical supply chains. Yet a new government organization or modifications to existing agencies may not be the answer. A consortium or non-profit may be better positioned to execute this mission on behalf of the government. As the data on supply chains improves and the government begins to learn lessons in this area from actions related to the medical supply chain, it should consider a more strategic and lasting solution beyond the initial steps it has taken to expand the DFC's mandate.

Proposed Executive Branch Action

Create a fusion cell of representatives from the Departments of State, Defense, and Commerce, the U.S. Trade Representative, the Small Business Administration, export promotion agencies, and others as needed to focus on supply chain reshoring and resilience. Conduct an analysis of alternatives for organizations to lead domestic supply chain reshoring by drawing on expanded authorities and financial incentives, to include government agencies, consortia, and nonprofits.

[556] Rush Doshi, *The United States, China, and the Contest for the Fourth Industrial Revolution*, Brookings (July 31, 2020), https://www.brookings.edu/testimonies/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution/.

[557] Id.

[558] Id.

[559] Timothy Meyer & Ganesh Sitaraman, *It's Economic Strategy, Stupid: The Case for a Department of Economic Growth and Security*, American Affairs (Spring 2019), https://americanaffairsjournal.org/2019/02/its-economic-strategy-stupid/; *Executive Summary*, American Compass (June 8, 2020), https://americancompass.org/essays/moving-the-chains-executive-summary/.

Part IV: A Technology Competitiveness Council: Logic and Options

The central role of emerging technologies in strategic competition and national economic competitiveness forces the United States to confront the reality that it is not organized for victory. This is not a crisis or country specific problem solvable with an ad hoc innovation like a Special Envoy, Czar, or Tiger Team. Plussing up existing organizations with technical expertise—including the National Security Council (NSC)—will not resolve the challenge: how to make technological competitiveness an orienting principle of strategy.

The United States needs a comprehensive technology strategy overseen by a strong executive to ensure continued leadership across the emerging technologies that define the future of strategic competition. An entity within the White House must be empowered to elevate technology concerns to the President, determine priorities, coordinate policies across departments and agencies, integrate national security, economic, and technology considerations, bridge the private-public divide, and shape a unified strategy.

Part IV presents a range of options focused on two courses of actions. First, Plus-Up one of the existing White House entities such as the NSC to drive emerging technology policy. Second, establish a new Technology Competitiveness Council led by a strong executive to elevate technology policy.

Landscape

National Technology Competitiveness as an Organizing Principle. The United States is on new strategic terrain. For the first time in a generation it confronts a serious strategic competitor in China. For the first time since the advent of the atomic age and rocketry, it faces transformative technologies—enabled by artificial intelligence—dramatically accelerating all elements of the competition. For the first time since becoming a global power, it faces a rival with the economic scale and technological prowess to challenge U.S. leadership and ambition across military and economic spheres. For the first time ever, it must manage a competition with a strategic rival enmeshed in its domestic economy and research and development enterprises. As a practical matter, this complicated landscape elevates emerging technology considerations across all facets of national policy while simultaneously increasing the importance of technology policy itself.

A Stronger Government Role in Innovation. The United States Government is now forced to rethink its role in the national competitiveness equation, the nature of the government's responsibilities for shaping private sector technology developments, and the relationship between industry and government. The United States Government cannot and should not try to centralize technology or economic policy by "nationalizing" anything, but it must exert more strategic control over the direction of innovation informed by national security considerations. The government will have to orchestrate policies to promote innovation, protect critical industries, and incentivize domestic research, development, and production across a range of critical technologies deemed essential for national security and economic prosperity.

A Constellation of Technologies. The orchestration is complicated by the fact that many of the emerging technologies central to the competition are still in their infancy. The real impacts of AI, biotechnology, and 5G networks are only now being seen. The impact of hypersonics and quantum computing are only beginning to be imagined. The interrelationship of the technologies adds another layer of complexity to the equation. AI will enable many associated technologies, while the full integration of the entire stack of emerging technologies will create entirely new possibilities for everything from waging war to eliminating diseases. The trajectory of their development, how they will be applied, and who will apply them first remain open questions. The government needs a plan for which technologies to prioritize for what purposes, and how to integrate multiple emerging technology strategies in an overarching vision for ensuring long-term American competitiveness and leadership.

The "Everything Matters More" Problem. Today's situation is unique. Each center of White House power—the NSC, the National Economic Council (NEC), and the Office of Science and Technology Policy—has a legitimate claim to leading a national competitiveness strategy centered on technology developments. In the past, one could more easily imagine which part of the White House might be *primus inter pares*. For instance, in the early Cold War, at a point of maximum danger, economic and technology policy could be subordinated to narrow national security concerns and the NSC could lead. In the post-Cold War, the promise of free markets and the end of conventional threats could plausibly elevate economic and trade concerns to the primary locus of power, and NEC could lead. In theory, the centrality of technology today could make the Office of Science and Technology Policy (OSTP) the place to focus a new strategy.

What is being considered here, fundamentally, is who will design, implement, and monitor a new strategy for national competitiveness. The answer must begin by defining the challenges of the current landscape and enumerating the missions necessary to design a strategy and implement a successful policy.

Dilemmas of the New Age. The complexity of the competition creates a series of dilemmas in the crafting of policies at the intersection of economics, security, and technology:

1. How to compete with a rival without compromising U.S. values—including free market principles, individual liberty, and limited government.

2. How to ensure the proper balance between defense and economic priorities.

3. How to preserve hardware advantages without suffocating the domestic designers and producers that rely on foreign competitors' markets.

4. How to capitalize on and shape private sector developments for national security ends without stifling private sector-led and free market innovation.

5. How to draw on the best global talent without creating dependencies on foreign expertise or enabling damaging technology and knowledge transfer to competitors.

6. How to foster an open collaborative research environment while closing licit and illicit loopholes exploited by foreign competitors

7. How to sustain long-term strategies for research and development that are nevertheless responsive to rapidly shifting short-term geopolitical and technology developments.

8. How to ensure the free flow of investment/capital without allowing strategic competitors to buy strategic advantage.

There are no clear ways to resolve these dilemmas. Crafting policies will require recognition of trade-offs in different courses of actions; clear acknowledgement of risks of different choices; and supplemental policies to offset the costs of chosen actions.

Missions: To prepare for this new terrain, the United States Government will need to:

1. *Analyze* technology trends and assess the relative competitiveness of U.S. technology sectors in relation to strategic competitors. (Horizon Scanning)

2. *Identify* and *Prioritize* sectors critical for the long-term resilience of U.S. innovation leadership across design, manufacturing, supply chain, and markets. (Mobilization/Critical Priorities)

3. *Create* a neutral forum for balancing national security, economic, and technology considerations across research, development, commercial interests, and national security applications. (Honest Brokering/Reconciling)

4. *Develop* domestic policy incentives (e.g. tax incentives, subsidies, government contracts) to sustain an innovation economy and develop specific, high-cost sectors like microelectronics or telecommunications necessary for long-term national security ends. (Techno-Industrial Promotion)

5. *Enact* tailored policies to protect U.S. and allied leadership in critical areas through targeted export controls and investment screening and counterintelligence activities. (Protect)

6. *Expand and Prioritize* domestic research and development in areas critical to national security, necessary to sustain U.S. leadership, and fill gaps in basic and applied research where the private sector does not focus. (Research)

7. *Implement* wide-ranging talent programs to grow the farm team of AI-talent in the United States and attract the best foreign talent, and then create better mechanisms to enable that talent to serve their country. (Talent)

8. *Build a high-level forum* for the private sector to begin engaging with the government on emerging technology policy, share threat information, express policy concerns, and develop partnerships. (Public-Private Partnership)

9. *Develop* international partnerships to reinforce domestic policy actions, shape international order, build markets, engage in research, and create an overall

environment that reflects American values and protects U.S. interests. (Coalition Building)

10. *Synchronize Budgets and Strategies* through a top-down process that reconciles short and long term priorities and links agency, White House, and congressional budget cycles to policy goals. (Investing to win)

Basic Organizational Needs

The broad outlines of the organizational requirements are largely enduring. The United States Government must be able to 1) convene the decision-makers with executive authority (the Principals) and present recommendations to the President for decision; 2) develop and synchronize strategies across geographic and functional concerns and domestic and international divides; 3) reconcile priorities within budget realities in short and long-term timeframes; 4) coordinate policy development across relevant departments and agencies; 5) coordinate and monitor policy implementation; and 6) analyze and forecast current and future trends.

The challenge of organization at the highest level comes down to three basic points:

1. **Only the White House can bridge the domestic-foreign divide.** Some cabinet agencies—e.g. the Departments of the Treasury and Commerce—can operate across the divide, but only in narrow sectors. None could do so across the complicated technology-economy-security landscape of today.

2. **Only the President commands.** Only the President, and in his place the Vice President, can reconcile interests across domestic and international concerns while balancing the economic and security concerns emanating from technology policy, and then exercise the authority to decide an issue. In theory, an Assistant to the President (e.g. the National Security Advisor) could exercise that power if empowered by the President. In practice, the Assistant to the President is challenged in wielding executive power as a proxy and few cabinet secretaries would accept the outcome.

3. **Setting the Agenda is Power.** Organizational power below the level of the President derives from the responsibility for framing the agenda, drafting the options, and structuring the policy deliberations for decisions. In theory, any of the Assistants to the President working with their respective staffs could play an "honest broker" role in teeing up policy debate. In practice, the respective staffs reflect the expertise, organizational culture, and priorities of their bureaucratic homes and the interests groups/industry they interact with, and tend to give more weight to their concerns in presenting issues.

Where is the United States now?

The United States Government possesses a weak executive structure for delivering a technology competitiveness strategy. The government will require a center of power that can exert gravitational pull on economic, national security, and science and technology policies. The United States has no such organization today.

Three separate White House Executive Office of the President (EOP) entities possess some responsibility and capacity to fulfill the basic organizational requirements. The NSC[560], The OSTP[561] and its associated National Science and Technology Council (NSTC)[562], and the NEC.[563] The Domestic Policy Council (DPC) also has critical related responsibilities and a similar mandate with leadership in the realm of immigration policy, education policy, and regulatory policy.[564] The Office of Management and Budget (OMB) oversees related budgets and government reform efforts.

In theory, any of these entities could be "plussed-up" to meet the requirements, perform the six basic tasks, take on the orchestration role, and achieve some of the missions outlined above. NSC, OSTP via NSTC, and NEC each have the necessary leadership rank, convening authority and council membership to hold policy deliberations chaired by the President. Each has a decision forum that includes the President, Vice President, relevant cabinet secretaries and the flexibility to include other relevant officials from within the White House and other parts of government. In fact, each has many of the same members. Each entity is led by an Assistant to the President—the highest rank of commissioned officer in the White House—with the possibility of a direct report line to the President. Each Assistant to the President is directed to coordinate their activities with the other relevant Assistants to the President and entities in EOP. Each entity also possesses a "staff" of agency detailees and political appointees serving similar functions. The "staff" serves the role of convening the lower-level interagency meetings, preparing meeting material, monitoring and analyzing policy developments, and staffing their principal. Staff power is a function of the power of its principal and the effectiveness and perceived legitimacy of the process it manages. It has no executive power, but it possesses the advantage of proximity to the President.

Recommendation 4.1: Empower a White House Entity and Senior Leader to Design and Implement a Comprehensive Technology Strategy.

The United States must strengthen executive leadership in technology policy in the White House by empowering a single entity to develop a comprehensive technology strategy for the

[560] The National Security Council has a statutory mandate to "advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the national security." 50 U.S.C. § 3021(b)(1).

[561] Pub. Law 94-282, National Science and Technology Policy, Organization, and Priorities Act of 1976 (1976), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/ostp_organic_statute.pdf.

[562] The function of the NSTC under the supervision of the Director of OSTP is to: "(1) to coordinate the science and technology policy-making process; (2) to ensure science and technology policy decisions and programs are consistent with the President's stated goals; (3) to help integrate the President's science and technology policy agenda across the Federal Government; (4) to ensure science and technology are considered in development and implementation of Federal policies and programs; and (5) to further international cooperation in science and technology. The Assistant may take such actions, including drafting a Charter, as may be necessary or appropriate to implement such functions." William J. Clinton, *Executive Order 12881—Establishment of the National Science and Technology Council* (Nov. 23, 1993), https://www.govinfo.gov/content/pkg/WCPD-1993-11-29/pdf/WCPD-1993-11-29-Pg2450.pdf.

[563] William J. Clinton, *Executive Order 12835—Establishment of the National Economic Council* (Jan. 25, 1993), https://www.govinfo.gov/content/pkg/WCPD-1993-02-01/pdf/WCPD-1993-02-01-Pg95.pdf.

[564] William J. Clinton, *Executive Order 12859 of August 16, 1993: Establishment of the Domestic Policy Council*, 58 Fed. Reg. 159 (Aug. 16, 1993), https://www.archives.gov/files/federal-register/executive-orders/pdf/12859.pdf.

United States. Such an entity would be responsible for integrating the technological, economic, and security aspects of each individual technology into a broader national leadership strategy. This is needed to ensure continued U.S. leadership across all emerging technologies, which are both inherently interconnected and will also define the future of strategic competition.

The Commission recommends creating a new Technology Competitiveness Council chaired by the Vice President with an Assistant to the President serving as the day-to-day coordinator (Course of Action 2 presented below). However, the Commission also presents a range of organizational models which could perform the necessary functions, and sees value in promoting public discussion about different models of executive-level technology leadership.

Course of Action 1: White House "Plus-Ups"

The obvious organizational solution would be for the President to make a concerted decision to strengthen one of the existing centers of EOP power, designate it the lead entity, allocate personnel and resources within EOP to reflect the new hierarchy, and have cabinet agencies buy-in to the new system. There are three options for how to do this:

Option 1a: NSC

If the strategic competition is framed foremost through the lens of threats, then the NSC could lead. It would have the organizational capacity to meld decisions about defense and intelligence capabilities, counter-intelligence actions, and the "protect" instruments—exports controls and sanctions. It has the legacy and muscle memory to move the United States Government on large endeavors and the largest of the three staffs. As a comparative point, the NSC is the only one of the three entities that actually functions as described in its mandate to coordinate policy under the supervision of the President. It has precedent, prestige, and 70 years of history behind it.

The national security advisor—by tradition more than law—enjoys a privileged position in White House decisions about security and international affairs.

- **Strengthening Emerging Tech in the NSC.** Minor organizational changes could bolster the NSC's tech capabilities. First, the NSC could establish a new Deputy National Security Advisor (DNSA) for Emerging Technology with the convening authority to lead a deputies-level workflow to drive the tech agenda. The DNSA could be dual-hatted as OSTP's Associate Director for National Security to draw in OSTP's technical staff. The DNSA could elevate policies through the Assistant to the President for National Security Affairs (APNSA) for major decisions in a traditional NSC Principals Committee hierarchy. The DNSA could be supported by an Emerging Technology Directorate within NSC to serve the secretariat function for emerging technology strategies and conduct its own policy analysis on a limited set of issues. Drawing on the expertise of the NSC's cyber, export control, weapons of mass destruction, intelligence, and regional staffs, the Emerging Technology Directorate would provide a locus of policy action with up to 15 direct and indirect support staff. It could further task and draw on the expertise of the other EOP entities and task studies, papers, and positions from the United States

Government. Economic integration could be handled by "dual hatting" an NSC economic official with NEC to "crosshatch" issues.

- **The Case against the NSC.** Elevating technology and economics within the NSC would overburden the APNSA who would still be responsible for carrying decisions to the President and wrangling Cabinet Secretaries. A new national technology leadership strategy—as mentioned above—would likely become one of many lines of efforts at the NSC rather than the organizing concept. Moreover, if the critical question is who frames the options, and who is responsible for elevating new issues to the principals, and who conducts the policy implementation work, then the NSC staff is not the most logical answer. Even an empowered NSC would not have the expertise or authority to weigh the critical domestic choices that a competitiveness strategy entails. The NSC lacks the expertise, domestic political role, or economic perspective to do the staff work to prepare the options for the economic dimensions of a competitive strategy. These functions, while critical for long-term national security, are inherently domestic. Even if economics were restored as a component of the NSC, which would be a prerequisite of an NSC plus-up, the NSC would not drive U.S. economic policy and there is no precedent for NSC having done so even when it had a large international economics directorate. Under the proposed arrangement, the NSC could influence S&T policy, but it would only marginally improve on OSTP's current role in R&D and perhaps overweight military investments for R&D, shape options that would put an excessive emphasis on "protecting" national security technology over open S&T collaboration and the economic benefits of international commerce, and prioritize the short-term benefits of strong centralized control instead of the long-term domestic risks of concentrated power.

Option 1b: OSTP

If the strategic competition is framed foremost as a long-term technology challenge and the critical issue is ensuring federal investment and policy to sustain innovation leadership, then OSTP could lead. It possesses the statutory mission for many of the critical tasks in ensuring that the R&D enterprise is funded and coordinated, possesses a mechanism for research protection coordination—the Joint Committee on Research Environments (JCORE)—and has the authority to lead in international partnerships for S&T. It oversees critical technology policies for AI, advanced manufacturing, nanotechnology. It maintains ties to academia and technology leadership in industry.

- **The Case for OSTP.** OSTP stewardship would ensure that long-term questions of research priorities, basic research, and the innovation ecosystem are primary concerns rather than afterthought in policy deliberations. OSTP at its core is an organization focused on promoting research and development. Its existing work shapes the many subordinate technology strategies and initiatives underway, convenes the relevant technical leaders of the United States Government to discuss research priorities via the National Science and Technology Council (NSTC), and it uses the JCORE to focus on foreign threats to U.S. technology. With clearer direction from the President, OSTP via the NSTC could take on the convening role it currently possesses but does not always exercise, while ensuring that technology consideration enjoys a leading role in agendas and deliberations. It could dual or trihat an Associate Director for National Security as DNSA for Emerging Technologies and NEC Deputy Director for International Economics.

- **The Case Against OSTP.** The demands of a new strategy exceed OSTP and the NSTC's focus on research and development. Elevating OSTP would give it operational and day-to-day responsibilities that it has never possessed across a range of issues it has only had an advisory role in the past. OSTP's umbrella of functions are critical to U.S. competitiveness, but it is a long-term focus and attention to basic rather than applied research represents just one element of technology policy. Its role in economic policy is even more tenuous than the NSCs, and its role in national security policy is largely advisory or limited to international engagement on narrow technical agendas. OSTPs national security expertise is technical not strategic and largely disconnected from the main policy efforts shepherded by the NSC. Moreover, given the diminished role of federal funding in driving emerging technology, the direction of federal resources will be less important than coordination and regulation (partnership) with the private sector which will run through either departments and agencies for particular projects or the NEC, Domestic Policy Council (DPC), and NSC for regulatory, legislative, and security issues.

Option 1c. NEC

If the competition is conceived foremost as an economic challenge, then NEC should lead. It could provide the bridge between national security concerns, long-term emerging technology policy, and an elevated and directed economic policy designed to restore domestic competitiveness while accounting for security concerns.

- **The Case for NEC.** NEC has the mandate to integrate domestic and international economic concerns and has strong ties to industry. NEC would be best positioned to weigh the complicated tradeoffs of pursuing greater government involvement in the economy and ensure security arguments are counterbalanced by private sector concerns and free market arguments. It is best positioned to develop the underlying economic analysis in partnership with the Council of Economic Advisors that should inform policy. NEC would be more sympathetic and attuned to business concerns and an important countervailing view to the over-securitization of innovation policy. NEC could dual hat the NEC deputy as DNSA for Emerging Tech and OSTP Assistant Director for National Security, allowing it to draw on the expertise of both NSC and OSTP staffs.

- **The Case against NEC.** Historically NEC has articulated the free-market, pro-free trade, limited regulation, pro-business, anti-regulatory views of the private sector. It may not be well-positioned to accommodate those views to the changing strategic landscape. Organizationally, it lacks an organized decision-making process for convening principals, and an organized process for orchestrating government-wide activities even if such a process exists on paper.

Bottom line on "Plus-Ups":

- None of the existing EOP organizations can achieve all of the objectives in their present configurations and each would be challenged to do so even with the addition of more resources, people, or "authorities."

- The organizational problem is basically identical no matter which entity is "plussed up." At least three power centers within the White House with nearly identical structures but three very different missions and priorities each have critical roles to play in the new strategic terrain.

- Any decision to elevate one of the organizations would necessarily diminish the power and responsibility of the other entities while exacerbating the predictable personality-driven dynamics that define reality in every White House.

- Any effort to reinvent or remove authority from existing coordinating bodies would likely layer or replicate whatever deficiencies exist in the current structure. Staffing adjustments, which could only be minor within EOP, would not dramatically change the capabilities of any of these organizations.

Course of Action 2: A New Technology Competitiveness Council and Executive (Commission Recommendation)

If National Competitiveness underpinned by technology development is the organizing principle of strategy, then NEC, NSC, and OSTP, must cede elements of their portfolios and subordinate some of their missions to a technology-centric body.

A coordinating body within one EOP organization that deals with core competencies of another EOP organization will be ignored by the organization that sees the function as a core mission. Each entity's policy process can produce an internally coherent recommendation, but it also risks producing incoherent approaches across the interagency processes and critical issues—like 5G—could be missed entirely.

In the absence of an overarching structure, it is now left to the President and Vice President to identify, adjudicate and reconcile the positions that emerge from the three parallel interagency processes, while leaving endless room for gadflies to try to run the gaps and influence the President. The President, in short, needs a tool for helping him decide and drive a new strategy down through the necessary-but-not-sufficient existing Councils into the rest of the government. The Commission proposes creating a Technology Competitiveness Council, led by the Vice President and with a Commissioned Assistant to the President as the day-to-day coordinator, to fill this role.

A Technology Competitiveness Council. A new Technology Competitiveness Council would treat economics, technology, and security as equally important considerations, and adjudicate the balance between them on a case by case basis but within an overarching strategy. It would ensure the critical missions outlined above are performed within a White House and Interagency context, and ensure that gaps between NEC, OSTP, and NSC responsibilities are filled and linked to OMB. It would not replace the NSC, NEC, or OSTP-led NSTC structures, but ensure a forum existed for reconciling different priorities, aligning purpose and budgets, and elevating technology concerns that would otherwise struggle to get high-level attention.

Council Membership would be the same amalgamation of EOP leaders and Cabinet Secretaries with an emphasis on the technology leadership.[565] The prerequisite for success is the President's determination to use such a vehicle to drive policy and arrive at decisions.

Leading the Technology Competitiveness Council. The new council would need executive leadership to remove the burden from the President and perform the basic council tasks. The leadership would also need to have an effective relationship with the Assistants to the President and the respect of the cabinet secretaries to prevent end-runs to the President, the establishment of shadow processes, and to ensure most disagreements are resolved short of presidential decision.

The Vice President as Chair. The Vice President could play the role of chair of a new Council—not unlike the role played by the Vice President in the Space Council. The Vice President exercises the authority to direct Assistants to the President and cabinet secretaries to act, signals the elevation of a new hierarchy of national priorities, and is capable of weighing the political dimensions of choices. The Chair role would require a commitment by the Vice President to serve a more substantial executive role than many Vice Presidents have served. Many prefer to serve as "counselor" and surrogate rather than administrator. The seriousness of the issue compelling the new organizational construct suggests that the coordinator role requires a seriousness of attention and purpose that not all past Vice Presidents would have sought or been able to fulfill.

A Commissioned Assistant to the President for Emerging Technology as Day-to-Day Leader. The President should commission an Assistant to the President to advise the Vice President and President, and coordinate the day-to-day policy and stewardship of the papers, meetings, and dispute resolutions that might emerge. This advisor would serve as the "honest broker" at the nexus of the APNSA, Director of OSTP, and NEC Director's responsibilities. A commissioned Assistant to the President is important because without it, the burden would reside with the Vice President or President to hear and resolve the other Assistants to the President's perspectives on every issue. An executive without the rank of Assistant to the President would be trampled by the other Assistants to the President. The Assistant to the President for Emerging Technology would need strong ties to the private sector technology community, understand the levers of government power, and enjoy a close relationship to the President. They could not merely be a Chief Technology Officer or Chief Information Officer. They would synthesize technology considerations, security concerns, and private sectors trends into a coherent strategy.

Staffing Considerations. The size of the staff of the technology executive will also determine the organization's bureaucratic flexibility and analytical capabilities. A small staff (less than five) would be necessary to staff the paper flow, prepare for meetings, and provide direction to the OSTP, NSC, and NEC staffs that would actually perform the lion's share of the work. There would be no "Policy Coordinating Committee"-like responsibilities for the

[565] Within EOP: White House Chief of Staff, APNSA, NEC Director, OSTP Director, U.S. Trade Representative, Office of Management and Budget Director. Cabinet Agencies: State, Defense, Treasury, Commerce, Homeland Security, and Office of the Director of National Intelligence. Plus, other leaders as directed by the Chair for relevant meetings—e.g. NSF director, DARPA director, etc.

staff, which would still be delegated to the existing NSC, NEC, and OSTP processes based on the agreement of the Technology Council. The Staff could in very limited cases fulfill a critical analytical role in ensuring disparate technology, economic, and security strategies were sequenced and aligned, highlighting potential gaps between strategies, and elevating any problems through the Assistant to the President for Emerging Technology to the Chair and Council for deliberation

In contrast, a larger staff would give the Technology executive, regardless of placement, increased power to control the trajectory of policy through the convening function and the ability to conduct more of its own policy analysis. A larger staff could convene interagency meetings, lead agenda setting, and drive policy implementation. This empowered staff (less than 15) would draw on an amalgamation of staff from the NSC, NEC, OSTP, and appointees.

Alternative Options for Day-to-Day Coordinator. The Commission considered several options for day-to-day leadership of the Technology Competitiveness Council. Although it recommends that a Commissioned Assistant to the President fill this role, as described above, the following organizational models are possible alternatives.

An Executive Secretary as Day-to-Day Coordinator. One alternative to a commissioned Assistant to the President "Coordinator of Coordinators" would be a non-commissioned Executive Secretary for the Council that would essentially serve as the process coordinator on behalf of the Chair (the Vice President) for the day to day interactions with NSC, OSTP, and NEC. An executive secretary functioning as a technocrat would avoid the proliferation of Assistants to the President, ensure the other Assistants to the President retained direct relations with the Chair and ensure the honest broker role of the coordinator was fulfilled without the empire building phenomenon of throwing another high-powered Assistant to the President into the White House equation.

A Deputies-Level Coordinator. A second alternative would be to establish a tri-hatted Deputy-level coordinator who would run the day-to-day work on behalf of the chair and integrate the ongoing emerging technology work of the three Councils. The Deputy would fill the role of NSC DNSA for Emerging Technology, OSTP Associate Director for National Security, and NEC Assistant Director. In this option, the coordinator could run a separate Deputies-level process with relevant departments and agencies to prepare for Council meetings. The Council meetings could then be co- or tri-chaired by the Assistants to the President or led by the Vice President as Council Chair. In theory, such a deputies-level coordinator/process could also exist without an overarching Council if it could feed recommendations through one of the Assistants to the President and existing Councils for presidential decision (see plus-ups section above).

Course of Action 3: The Technology Envoy

For a White House loath to create more councils or processes but still determined to elevate technology concerns, the creation of an Assistant to the President for Emerging Technology could be a minimal investment yielding high return. The right person—connected to the President, experienced with industry, familiar with tech trends and government levers, and respected by the rest of the EOP leaders and cabinet members—could be a force multiplier. They could sit in any relevant White House meeting to inject technology perspectives, advise the APNSA or NEC director, and counsel the President and Vice President. Such a person would enjoy a panoptic view of White House policy development across domestic and international divides and be able to detect seams, gaps, and opportunities. They would be unencumbered by process or managerial responsibility. They could end-run broken processes and inject new ideas directly into the policy bloodstream. The disadvantage of such a technology envoy would be the position's total dependence on personal relationships to achieve effect. Without ownership of a process or convening power, even a commissioned Assistant to the President can be quickly marginalized if they do not add value to colleagues and enjoy—and be seen to enjoy—access to the President.

Conclusion

The challenges of integrating and elevating technology concerns with security and economic developments represents a substantial strategic gap that must be filled. If the President is willing to prioritize the technology competition, then a stronger executive structure led by an empowered individual could play the crucial role in shaping a new strategy.

TAB 5 — Marshal Global AI Cooperation & Ethics

An Operational Framework for Global AI Cooperation

The scope and strength of U.S. alliances and partnerships have historically provided the United States with an asymmetric advantage over its strategic competitors. These resilient relationships, borne out of America's commitment to a rules-based international order and diplomacy, led to victory in World War II (WWII), establishment of an international framework based on rule of law—reflected in the United Nations and other international institutions—and defeat of the Soviet Union. They have limited nuclear proliferation, provided international legitimacy and capabilities for coordinated military actions, such as the Coalition to Defeat the Islamic State of Iraq and Syria, and enabled a global economy through cooperation and innovation.

General Eisenhower attributed victory in WWII in large part to the "intangible element" of teamwork among the Allies.[566] Testifying before Congress as the United States embarked on one of the greatest international rebuilding projects, Secretary of Defense George Marshall explained that U.S. strength depends on the "strength of its friends and allies. Although the United States is strong and has great resources it would be unwise for the nation to rely solely upon its own strength. The most effective and least costly means of insuring [sic] peace is through mutual aid and collective security arrangements with U.S. allies."[567]

This vision was reinforced throughout the Cold War by every U.S. administration. In 1963, President John F. Kennedy sent a letter to French diplomat and economist Jean Monnet which reaffirmed that since WWII "the reconstruction and the knitting together of Europe have been objectives of United States policy" recognizing that "a strong Europe would be good not only for Europeans but for the world."[568] In 1989 remarks in Germany, President George H. W. Bush described North Atlantic Treaty Organization (NATO) as "a way for Western Europe to heal centuries-old rivalries, to begin an era of reconciliation and restoration."[569]

Since the end of the Cold War, globalization and emerging technologies have generated stark inequalities as political, economic, and military power have become more widely dispersed. The emergence of great power competition with Russia and China has required the United States to reform its national security institutions to effectively compete without an overreliance on outdated military approaches.[570]

[566] Remarks by Dwight Eisenhower, Chief of Staff of the Army, delivered at the Cleveland Aviation Club, (Apr. 11, 1946), https://www.eisenhowerlibrary.gov/sites/default/files/file/pre_presidential_speeches.pdf.

[567] Mark A. Stoler & Daniel D. Holt, *The Papers of George Catlett Marshall: "The Man of the Age"*, John Hopkins University Press Vol. 7 at 598, (2016).

[568] Letter from John F. Kennedy to Jean Monnet Commending His Achievements on Behalf of European Unity (Jan. 22, 1963), https://www.cvce.eu/en/obj/letter_from_john_f_kennedy_to_jean_monnet_23_january_1963-en-c0534caa-573c-478a-a07f-487086438dfa.html.

[569] George H. W. Bush, *Remarks to the Citizens in Mainz: A Europe Whole and Free* (May 31, 1989), https://usa.usembassy.de/etexts/ga6-890531.htm.

[570] Robert Gates, *The Overmilitarization of American Foreign Policy,* Foreign Affairs (July/Aug. 2020),

The United States' enduring relationships with allies and partners represent asymmetric advantages over competitors and adversaries. Those relationships are, today, as essential in the terrain of artificial intelligence (AI) and emerging technology as they are for military strategy. U.S. national security faces new threats which it must confront with U.S. allies and partners, based on shared values and tangible ways to prevail over threats from authoritarian regimes. AI will provide capabilities to identify those challenges along with opportunities that will allow democratic nations to respond to such conditions faster and more effectively. Organizing diplomatically around world-changing technology will build the resilience of those alliances and partnerships to address common threats in other contexts.

The United States must pursue a comprehensive approach to strategic competition, which requires investments in diplomacy and development, institution building, and modernized military capabilities with new operational concepts for long-term competition below the threshold of military conflict. Building upon the Commission's prior recommendations focused on the Five Eyes alliance and reorienting the Department of State, the Commission proposes an operational framework for global AI cooperation. The framework has three pillars, each of which requires clear, sustained U.S. leadership to establish and maintain:

I. Deepening Global AI Coordination for Defense and Security

The United States must deepen its defense and security relationships to improve the development, adoption, and deployment of AI systems across the range of military and security applications. The Commission focuses on NATO as an essential component of U.S. national security and makes recommendations to address the significant challenges—and opportunities—that AI poses to NATO operations.

II. Shaping AI Cooperation through Multilateral Forums

The United States can shape the future of AI, fostering effective, multilateral coalitions around critical issues. To do so, the United States must take a proactive role in multilateral institutions while also building stronger alliances with democratic nations. The Commission offers an assessment of the multilateral landscape and recommendations to guide U.S. diplomacy through a "coalition of coalitions" strategy. The Commission also proposes ways to enhance U.S. posture in development of technical AI standards.

III. Building Resilient Bilateral AI Cooperation with Key Allies and Partners.

AI and associated technologies will be instrumental for shared prosperity and security among the United States and its allies and partners. The Commission recommends a strategy for engaging key allies and partners in the Indo-Pacific region—centered on India—and with the European Union. The strategy includes a Blueprint for AI Cooperation (see Annex B) designed to improve the resiliency of U.S. alliances and partnerships. The Blueprint includes guidance on concrete, operational projects, applications, and implementation mechanisms for collaborative

https://www.foreignaffairs.com/articles/united-states/2020-06-02/robert-gates-overmilitarization-american-foreign-policy; Nadia Schadlow, *The End of American Illusion*, Foreign Affairs (Sept./Oct. 2020), https://www.foreignaffairs.com/articles/americas/2020-08-11/end-american-illusion.

AI work in critical areas —work that will further AI consistent with democratic values and strengthen the ties that connect the United States with its allies.

Pillar I: Deepening Global AI Coordination for Defense and Security

The Departments of State and Defense (DoD), with support from Congress, must take steps to deepen U.S. defense and security alliances to address the geopolitical challenges associated with AI in an era of algorithmic warfare and support U.S. national security interests.[571] It must do so in a manner consistent with the law of war, the rule of law, and the values and norms that are a bedrock of U.S. democracy.

In the Commission's *First Quarter (QI) Recommendations memorandum*, it focused on ways to improve AI cooperation among key allies and partners in the national security context by establishing a National Security Policy Framework for AI Cooperation and pursuing AI-related military concept and capability development with allies and partners, beginning with a focus on the Five Eyes alliance.[572] The Commission observed that AI presents significant challenges for military interoperability that impacts the effectiveness of military coalitions—and that developing interoperable systems is an opportunity and challenge across U.S. alliances.

In this report, the Commission is proposing methods to enhance the development and integration of AI-enabled technology throughout military systems and operations, first within NATO and then within the context of other international defense and security partnerships.

Issue 1: Furthering NATO's Adoption of AI

During the last 70 years, the United States has played a leading role in sustaining and adapting NATO to new challenges. The Alliance remains a foundation for U.S. national security. Liberty, prosperity, and collective security are at the core of this relationship.

Increasingly, NATO and its member states recognize that AI-related technology has transformative potential for defense and security.[573] In this age of algorithmic warfare,[574] however, differential adoption of technology among member states and corresponding challenges around interoperability threaten to undermine NATO's effectiveness. Coordinated, accelerated, and responsible adoption of AI must be an urgent priority across the Alliance. NATO and its member states need to dedicate personnel and resources to develop interoperable technology and undertake operations reliant on advanced technology. NATO and member states have begun a concerted effort to address the AI imperative, and the need to adopt Emerging and Disruptive Technologies (EDT) more broadly. This has

[571] *Interim Report*, NSCAI at 10 (Nov. 2019), https://www.nscai.gov/reports.

[572] *First Quarter Recommendations*, NSCAI at 64-67 (Mar. 2020), https://www.nscai.gov/reports.

[573] *London Declaration*, NATO (Dec. 4, 2019), https://www.nato.int/cps/en/natohq/official_texts_171584.htm; *Science & Technology Trends 2020-2040: Exploring the S&T Edge*, NATO Science & Technology Organization (Mar. 2020), https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

[574] Deputy Secretary of Defense Robert O. Work, *Memorandum: Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)* (Apr. 26, 2017), https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf.

included the October 2019 adoption of a NATO EDT Roadmap by Allied governments; creation at NATO Headquarters of two new staff teams—the Innovation Unit and the Data Policy Unit—as well as a senior-level Innovation Board; and launching of an Advisory Group of external experts on EDT. An Artificial Intelligence White Paper was produced and submitted to Allied governments in July 2020, with proposals for five-year goals for AI development, adoption, and deployment, as well as for the development of an overarching AI implementation strategy. An additional staff White Paper on Autonomous Technologies is expected later in 2020. Subject to confirmation by Allied governments, NATO staff expect the development of a NATO Data Exploitation Framework Policy and a NATO Artificial Intelligence Strategy in the course of 2021.[575]

Ultimately, NATO and its member nations must develop and incorporate AI, facilitated by seamlessly enabling infrastructure, across the range of enterprise, mission support, and operational AI applications.[576] These applications include the following: joint all domain command and control; force management and planning; early warning and detection; ballistic missile defense; intelligence, surveillance, and reconnaissance; humanitarian and disaster relief; predictive maintenance; and military mobility.

To achieve this, the Alliance and Allied governments must address unique challenges that AI presents. First, rapidly evolving technology means that NATO must pursue AI-related development and adoption with support from more technologically advanced member states. NATO has begun including AI-related experimentation in its exercises.[577] This should be accelerated to avoid losing pace with the leading edge of commercial innovation in the United States, as well as the rapid progress by adversaries on AI-related technology development and application. Unabated, current trends will expose NATO to increasing strategic and military risk. Because of the commercial nature of AI-related technology and the backdrop of geopolitical competition, this is not simply a question of defense spending, but also a matter of configuring the appropriate coalitions and partnerships within NATO to align technology and technological know-how with operational needs. A significant aspect of this is drawing on the expertise and resources of member states like the United States.

In addressing the unique challenges of AI, attention must also be focused on responsible development and use. To further the responsible use of AI, preliminary staff work at NATO is focused upon building on AI principles, including those adopted by the DoD and those published by other allies. While this is a step towards reaching responsible AI consensus among its members, NATO's 30 member countries each find themselves at varying phases of AI maturity. Thus, efforts to align NATO members on the next step of operationalizing AI principles, such as adopting common standards for traceability, interpretability, safety, and security of AI systems, will be necessary but challenging. Alignment on documentation standards, for instance, is critical for future interoperability, sharing of data and models, and general cooperation among allies.[578] U.S. coordination with NATO is critical to help

[575] NSCAI staff interviews with U.S. NATO and NATO International Staff (July 17, 2020; July 30, 2020; Sept. 21, 2020).

[576] Danielle C. Tarraf, et al., *The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations*, RAND Corporation at 25-27 (2019), https://www.rand.org/pubs/research_reports/RR4229.html.

[577] See, e.g., Patrick Tucker, *How NATO's Transformation Chief is Pushing the Alliance to Keep Up in AI,* Defense One (May 18, 2018), https://www.defenseone.com/technology/2018/05/how-natos-transformation-chief-pushing-alliance-keep-ai/148301.

[578] See, e.g., Erik Lin-Greenberg, *Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making*, Texas National Security Review at 71-72 (Spring 2020), http://dx.doi.org/10.26153/tsw/8866/ (noting that "[t]o

NATO members align on foundational AI principles as well as the common practices that should be prioritized to operationalize them.

Second, pursuit of increasingly advanced technology across operations, from logistics to warfighting, will only increase the need for highly skilled technical experts. NATO, like defense departments and ministries of member states, is competing with the private sector for the same talent and lacks agility to ramp up expertise and talent to address urgent needs.[579] NATO bodies require more flexibility to enhance in-house expertise through hiring, training, and mobility measures, and to access external sources of expertise.

Third, differential expertise and adoption across the Alliance creates interoperability risk. NATO and member states have made initial progress on data fusion, data exploitation, pilot projects, and experimentation to address differentials across the Alliance. These efforts hold promise and will generate important learning about not only AI-related methods, but also associated issues for data sharing, training, and contracting underlying AI adoption.

Recommendation 1: The Departments of State and Defense should provide clear policy guidance and resource support to NATO's AI initiatives by aligning resources and providing technical expertise to assist NATO in its adoption of AI to achieve:

- Accelerated development and adoption of operational practices to implement overarching AI principles and enable incorporation of AI-related technologies;
- Coordination of data sharing practices with a focus on privacy-enhancing technologies and methods;
- Development of NATO's technical expertise;
- Adoption of technical standards and architectures to promote interoperability; and
- Implementation of simulations, wargaming, experimentation, and pilot projects to develop use cases for data fusion, data exploitation, and interoperability across the Alliance.

Development and implementation of AI tools and techniques can further NATO's mission by generating greater predictive and analytical insight for decision makers at the North Atlantic Council and enhancing the credibility and sustainability of deterrence. The ability of NATO to incorporate AI into its military and humanitarian operations requires political will

ensure alliances and coalitions are able to leverage AI technologies during their operations, states will need to remove barriers to data sharing and access," and discussing first steps).

[579] Christie Lawrence & Sean Cordey, *The Case for Transatlantic Cooperation*, Harvard Kennedy School Belfer Center at 44, 126 (Aug. 2020), https://www.belfercenter.org/sites/default/files/2020-08/TransatlanticAI.pdf (citing Acting Director of the JAIC Nand Mulchandani).

among Allied governments and strong coordination to develop a common operating picture, develop and apply AI across applications, bolster multinational force development and planning, and stress test decision making procedures.

Accelerated development and adoption of operational practices to implement overarching AI principles and enable incorporation of AI-related technologies. While the United States Government, Allies, and the NATO Alliance should have flexibility to determine alignment priorities based on their evolving needs, preferential weight should be given to three key areas that will be critical in the near- and long-term: aligning on documentation requirements and intended use;[580] establishing confidence in 'systems of systems';[581] and ensuring system robustness and reliability,[582] with a focus on mitigating adversarial attacks.[583]

As the Departments of State and Defense work with NATO and member states to develop NATO's AI program, they should elevate DoD's principles and supporting practices to shape joint initiatives for responsible AI at NATO. At the same time, they should leverage the Commission's *Key Considerations for the Responsible Development & Fielding of AI*[584] as a resource for implementing commonly agreed upon AI principles.[585] The *Key Considerations* provide an ontology of concerns and opportunities that the Departments of State and Defense and NATO can use to reach common ground on priorities for developing and responsibly using AI for defense and security. They represent a synthesis of practices and

[580] Common documentation requirements (for data, models, and systems) are a prerequisite for fostering trust in AI systems of allies and for allowing NATO members to share information and possibly AI tools more quickly. For instance, only by employing common documentation requirements (e.g., documenting origins of data) can NATO members readily assess an AI system (e.g., assessment of interoperability of systems, fitness for use, ability to integrate/compose well, and compliance with various national requirements and constraints). Common documentation standards would be a key enabler to trusted data sharing and subsequent data exploitation. Arriving at a documentation approach that works for 30 nations will take early, coordinated effort.

[581] AI-intensive systems introduce opportunities and challenges for emergent system performance (i.e., the consequences of the interactions and relationships among system elements, rather than the independent behavior of individual elements). Given the need to establish and preserve justified confidence in the performance of AI systems, attention must be paid to the potential for undesired interactions and emergent performance as AI systems are composed. As the U.S. increases its use of AI-intensive systems, including through ad hoc opportunities to integrate systems with allied AI-intensive systems, the U.S. and its allies should make emergent system behavior an important topic for coordination. Indeed, multi-agent systems are being explored and adopted in various domains, as are swarms, fleets, and teams of autonomous systems. Given this context, future research and development (R&D) is needed to develop a better understanding of how to conduct TEVV; to increase the ability to have confidence in emergent performance of composed AI systems; and to better understand interacting AI systems ("multi-agent scenario understanding").

[582] In the *Key Considerations*, the Commission noted that future R&D is needed to advance capabilities for AI security and robustness—to cultivate more robust methods that can overcome adverse conditions; advance approaches that enable assessment of types and levels of vulnerability and immunity; and to enable systems to withstand or to degrade gracefully when targeted by a deliberate attack.

[583] As noted in the *Key Consideration*s, to address intentional and unintentional failures, ongoing work is needed to expand notions of adversarial attacks to include various "machine learning attacks" (which may take the form of an attack through supply chain, online access, adversarial training data, or model inference attacks, including through Generative Adversarial Networks); seek the latest technologies that demonstrate the ability to detect and notify operators of attacks, and also tolerate attacks; incorporate advances in intentional and unintentional ML failures; and adopt a security development lifecycle for AI systems to include a focus on potential failure modes.

[584] See *Key Considerations for Responsible Development & Fielding of Artificial Intelligence*, NSCAI at 7-14 (July 22, 2020), https://www.nscai.gov/reports [hereinafter, *Key Considerations*].

[585] Id. A preliminary effort to list relevant principles includes the following: *Lawful*, *Responsible*, *Equitable*, *Traceable*, *Reliable*, *Governable*, *Secure*, and *Interoperable*. The list is intended to provide a starting point for discussions at NATO. Allies are also considering broad principles of engineering good practice in order to build in compliance (by design) with core principles of governability and accountability.

actions to operationalize each of the AI principles adopted by the DoD in addition to other commonly cited AI principles.[586] Leveraging its own learnings and the *Key Considerations*, the United States has the opportunity to contribute to NATO discussions to operationalize commonly shared AI principles among allies, which in turn will lead to confidence and trust in respective AI systems amongst its members. The recommended practices and identification of areas needing future work in the *Key Considerations* offer a blueprint of technical, policy, and research areas that will need alignment for interoperability and shared trust between the U.S. and NATO members in the near- to long-term. Using this blueprint would permit the United States to contribute to setting the agenda for NATO members to achieve responsible AI development and use.

In addition, the Departments of State and Defense should apply U.S. expertise around the responsible use of AI-related technologies and autonomy in military systems. Autonomy raises challenging ethical and legal issues for the Alliance, which will need to articulate policy and the associated doctrine as part of an AI implementation strategy and associated efforts. As described below, a range of NATO initiatives provide entry points to accelerate development and adoption based on key considerations for responsible use, while promoting interoperability and common standards. The Departments of State and Defense should ensure that the initiatives effectively incorporate responsible AI considerations, opportunities, and lessons from the United States' experience and capabilities.

Coordination of data sharing practices with a focus on privacy-enhancing technologies and methods. The United States should assist NATO in developing coordinated data practices to enable collection, storage, use, and sharing of data across the Alliance. The policy should include coordination with regards to national laws, regulations, and multinational constructs such as the national security and defense exceptions to the European Union's (EU) General Data Protection Regulation (GDPR) to avoid unintended or counterproductive constraints on alliance flexibility to use data for collective security. Wherever possible, it should be NATO policy to recognize the importance of individual privacy and to develop and practice the necessary methods and approaches that preserve those privacy principles. It will be important to document national practices and legislation so that NATO can take appropriate measures with an understanding of national legal, regulatory, and administrative barriers to data sharing for defense and security applications. Alliance-wide political commitment to address the modalities of data sharing is important because it would imply a political responsibility of each Allied government to ensure the goals of the agreement could be negotiated within NATO and agreed by the North Atlantic Council. Members of the EU have a particular responsibility to ensure that their obligations to comply with EU data sharing laws do not prevent or constrain their full participation in data sharing in the NATO context. Moreover, NATO and the EU should collaborate on the development of privacy-preserving AI and machine learning technology to ensure compatibility.

The United States should advance top-down and bottom-up approaches toward an overarching Alliance data sharing policy. Top-down approaches would include at least three elements:

[586] See Annex C of this report.

- Ensuring that operational data generated in the context of NATO exercises is collected, stored, shared, and made exploitable across the NATO Enterprise, the Alliance, and among Allies;[587]

- Developing a common, shared, but not exclusive AI Hub to lead on data analytics and AI modelling activities; and

- Installing a Chief Data/AI/Analytics Officer with sufficient expertise to lead the AI Hub.

Bottom-up approaches can benefit from actionable U.S. (and allied) insights in the areas of data exploitation, AI, autonomy based on specific experiments, demonstrations, pilot projects and wargaming. In addition, the United States and Allies should explore coordinated R&D on privacy-enhancing technologies, common technical standards and frameworks, and development of potential AI and machine learning applications.

Development of NATO's technical expertise. The United States Government should examine avenues to train NATO personnel and recruit staff from the United States to bolster NATO's capabilities. The DoD should work with its NATO allies to pool their defense AI talent and bolster these actions through joint efforts. Specifically, the United States and NATO allies should explore coordination of joint training and educational programs, defense-related talent exchanges to increase NATO's AI expertise, talent secondments into industry, and best practices sharing.

Establishment of a NATO AI Hub would present an additional opportunity to develop technical AI expertise and support to senior leadership. The AI Hub should adopt methods to define and track AI talent in member nations. The United States and allies should evaluate options to enhance the AI Hub with new positions, voluntary national contributions and other external support from academia and the private sector. The Commission also notes the establishment of NATO's Data Policy Unit which would benefit—if not require—significant technical capacity that is aligned with the scope and depth of its mission and tasks to generate an Alliance data policy.

Adoption of technical standards and architectures to promote interoperability. Recognizing the different adoption rates of advanced technology among member states, NATO must pursue efforts to avoid a stark divergence between the United States and Allies which could hinder political cohesion and military effectiveness. AI-related technologies have potential to improve NATO capabilities for military and humanitarian operations, but if interoperability challenges are not resolved, they could also widen the capability gaps between larger and smaller allied nations.[588]

Implementation of simulations, wargaming, experimentation, and pilot projects to develop use cases for data fusion, data exploitation, and interoperability across the Alliance. Use cases, simulations, experimentation, and

[587] NATO standardization agreements can serve as a vehicle for developing common AI data standards. See *Standardization*, NATO (Jan. 23, 2017), https://www.nato.int/cps/en/natolive/topics_69269.htm.
[588] Erik Lin-Greenberg, *Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making,* Texas National Security Review (2020), https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/; Martin Dufour, *Will Artificial Intelligence Challenge NATO Interoperability,* NATO Defense College Policy Brief (Dec. 10, 2018), http://www.ndc.nato.int/news/news.php?icode=1239.

wargaming are urgently needed to develop an analytical foundation to clarify and manage the implications. NATO should conduct wargaming and experimentation in order to further develop use cases and agreement on specific underlying data sets; examine machine learning-related approaches to stress test capabilities and operational concepts; develop common Test & Evaluation, Validation & Verification (TEVV) procedures; ensure lifecycle data management—labelling, storage, accessibility, and security; and explore possibilities of privacy preserving machine learning (PPML) to overcome data protection, security, and privacy issues among allies and with partners. NATO already has vehicles and mechanisms for constructing pilot projects and conducting experimentation, such as maturing the NATO innovation hub to bring together NATO operational needs with commercial and academic expertise, leveraging the recently established Technical Advisory Group, informing NATO's human capital initiative, and, most importantly, defining and pursuing preliminary use cases.

Proposed Executive Branch Action

The Departments of State and Defense must engage with NATO and Allies immediately to contribute meaningful, concrete guidance in alignment with the recommendations set forth above in order to inform the efforts in early 2021 to build out a cohesive AI strategy. As part of this, the DoD should convey to NATO and Allied governments that AI is a top priority of the Secretary of Defense.[589]

To further the responsible use of AI among allies, the Secretaries of State and Defense should issue a memorandum encouraging the Departments of State and Defense, as they liaise with NATO, to emphasize critical areas from the *Key Considerations* as strategic priorities for NATO member alignment. The Departments should elevate areas across the *Key Considerations* document as appropriate, while giving particular weight and emphasis to achieving common documentation requirements; establishing confidence in 'systems of systems'; and ensuring robustness and reliability, including mitigating adversarial machine learning attacks and hardening allied AI-enabled systems.

In addition, the Departments of State and Defense should support high-level Alliance policy direction and identification of AI-related priorities, including by providing political direction, proposing use cases and operational needs, supporting NATO's access to expertise, and generating actionable learning and implementation of AI-related technology and methods through other NATO initiatives. Relevant initiatives include:

- *NATO 2030*, the Secretary General's effort to strengthen the Alliance for an increasingly competitive world.[590]

[589] See Secretary of Defense Dr. Mark T. Esper, *Remarks for DOD Artificial Intelligence Symposium and Exposition* (Sept. 9, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2341130/secretary-of-defense-remarks-for-dod-artificial-intelligence-symposium-and-expo/.

[590] NATO 2030 adopts a more global outlook, recognizing the importance of democracies such as Australia, Japan, New Zealand, and South Korea, while emphasizing the importance of emerging technologies and the norms and standards that govern them. See *Remarks by NATO Secretary General Jens Stoltenberg on launching #NATO2030 - Strengthening the Alliance in an increasingly competitive world*, NATO (June 8, 2020), https://www.nato.int/cps/en/natohq/opinions_176197.htm.

- *Deterrence and Defense for the Euro-Atlantic Area*, the Supreme Allied Commander Europe's military plan to address shortfalls in existing response capability, including emerging threats in space, cyber, and new technology for the Alliance.[591]

- *Warfighting Capstone Concept*, an overarching concept to guide Warfare Development for the Alliance's military instrument of power and the biennial Warfare Development Agenda informed by a twenty-year horizon warfighting perspective.[592]

- *EDT Roadmap*, part of the AI implementation strategy, along with other deliverables in technology areas such as autonomy and biotechnology.

- *NATO Science and Technology Strategy*,[593] which provides context for anticipating the potential development and impact of technology on future Alliance operations.

The Commission recommends further that the Departments of State and Defense propose including an Alliance AI Strategy deliverable as part of a possible NATO Heads of State Summit in the summer of 2021. An Alliance AI Strategy should include policy guidance to achieve NATO's AI aspirational goals along with implementation steps consisting of:

- Agreement on AI principles and ethics to govern NATO's development and use of AI;

- Alliance AI-related focus areas and associated metrics, drawing on work developed by the OECD.AI Policy Observatory;[594]

- Methods to leverage the NATO Science and Technology Organization to facilitate convergence between Allies research and development (R&D) priorities, while considering the work of civilian, multinational, and national research institutions;

- Goals to inform the NATO Defense Planning Process (NDPP) and allied inputs to ensure that capability targets include AI-related goals across national- and common-funded capabilities (including the relevant aspects for data exploitation, AI, and autonomous capabilities);

- Goals for AI capability development and defense planning cooperation between NATO and the European Defense Agency to ensure AI compatibility;[595]

[591] See *Virtual Conversation with NATO Deputy Secretary General Mircea Geoană with the President of the Brookings Institution, John R. Allen, in the EU Defense Washington Forum*, NATO (July 9, 2020) https://www.nato.int/cps/en/natohq/opinions_177110.htm?selectedLocale=en.

[592] The United States should ensure that parallel efforts such as the all-domain capstone warfighting concept are synchronized with, and inform NATO's parallel effort with key AI-related innovation and considerations for deterrence and warfighting challenges.

[593] *NATO Science and Technology Strategy: Sustaining Technological Advantage*, NATO (July 27, 2018), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20181107_180727-ST-strategy-eng.pdf.

[594] The OECD.AI Policy Observatory, discussed later in this tab, has generated a series of studies measuring AI development and adoption that may assist in development of NATO AI strategy. See *OECD Methods & Metrics*, OECD.AI (last accessed Oct. 1, 2020), https://www.oecd.ai/oecd-metrics-and-methods.

[595] See *Capability Development Plan*, European Defence Agency (Aug. 6, 2019), https://eda.europa.eu/what-we-do/activities/activities-search/capability-development-plan; *Capability Development and Defence Planning*, NATO (last accessed Oct. 2, 2020), https://act.nato.int/activities/allied-command-transformations-innovation/capability-development-and-defence-planning.

- Development of use cases and associated data sets across decision-making, military operational requirements, concepts, capability targets, standards, and enterprise operations;
- Efforts to incorporate AI-related aspects across common NATO standards through the Conference of National Armaments Directors and associated subgroups and informed by international normative and technical standards bodies;
- A plan for developing human capital, education and training;
- Collaborations with non-NATO partners, including industry and academia;
- AI-related information exchanges about blue and red capabilities and trends; and
- An assessment and evaluation of progress, to be reviewed bi-annually at the Ministerial level and by Chiefs of Defense, that would enable incorporation of lessons learned in to the NATO defense planning processes.

Lastly, the DoD should continue to support bottom-up partnerships, technical collaborations, and pilot projects with NATO elements that are already working on areas related to interoperability, data, human capital, and norms and standards.

Issue 2: Deepening Defense and Security AI Coordination with Partners & Allies Outside of NATO

It is also in the United States' vital national security interest to deepen AI-related defense and security cooperation with U.S. treaty allies and other key partners.

The Five Eyes nations remain the closest and most important U.S. allies and collaborators across the spectrum of AI development. The Five Eyes alliance has collaborated on Project Maven, the Pentagon's first AI program, as well as R&D and TEVV with defense arrangements like the Technical Cooperation Program's AI Strategic Challenge (TTCP AISC). The Challenge focuses on trustworthiness, rationalization, effective transition of AI technologies from science and technology to acquisition and users (coalition warfighters, commanders, and decision makers), and the intersection of AI and international law. The anticipated outcomes will provide the groundwork for multinational AI technology development and deployment into multinational operations.[596]

Yet technological advances such as artificial intelligence, machine learning, quantum technologies, and robotics will transform the future operational environment and will require the United States to strengthen its defense and security cooperation with countries beyond NATO and the Five Eyes alliance.[597] Indeed, there is potential to deepen the U.S. security relationship with key partners, as the Commission will explore in its final report.

To that end, the Commission welcomes the new effort by the DoD Joint Artificial Intelligence Center (JAIC) to launch the Artificial Intelligence Partnership for Defense (AI PfD). The AI PfD, comprising the United States plus twelve partner nations—Australia, Canada, Denmark, Estonia, Finland, France, Israel, Japan, Norway, South Korea, Sweden,

[596] *Interim Report,* NSCAI at 44-47 (Nov. 2019), https://www.nscai.gov/reports.

[597] *UK MOD Five Eyes Future Operating Environment 2040*, DCDC 2019 (unclassified portions).

and the United Kingdom—seeks to "provide values-based global leadership" on adoption of AI in the defense and security context.[598] At the first AI PfD meeting in September 2020, partner nations agreed that the AI PfD will "bring[] together like-minded nations to promote the responsible use of AI, advance shared interests and best practices on AI ethics implementation, establish frameworks to facilitate cooperation, and coordinate strategic messaging on AI policy."[599] Ultimately, the AI PfD may provide the space for democratic allies and partners to work through defense issues on AI. This effort should receive continued support from DoD and Congress and could serve as a primary coalition to expand AI cooperation on defense and security issues to a broader group of nations, including critical partners not included in formal security treaty alliances.

Recommendation 2: The Departments of State and Defense should negotiate formal AI cooperation agreements in the Indo-Pacific region with Australia, India, Japan, New Zealand, South Korea, and Vietnam.

In the Indo-Pacific region, a priority under the National Defense and Security Strategies, the United States is taking encouraging steps to strengthen conventional defense partnerships.[600] Speaking at the August 2020 U.S.-India Strategic Partnership Forum, Deputy Secretary of State Stephen Biegun announced the United States' desire to deepen and take advantage of increased opportunities for collaboration with Quadrilateral Security Dialogue ("Quad") partners India, Japan, and Australia, and nations like South Korea, Vietnam, and New Zealand committed to advancing a free and open Indo-Pacific region.[601] On October 6, 2020, Quad members held a ministerial meeting in Tokyo to discuss further defense cooperation. At the meeting, members discussed deepening cooperation on addressing challenges arising from COVID-19, promoting a stable and open Indo-Pacific, maritime security in the Indo-Pacific region, and the centrality of ASEAN in the region.[602] This

[598] AI Partnership for Defense, *Joint Statement* (Sept. 15-16, 2020), https://www.ai.mil/docs/AI_PfD_Joint_Statement_09_16_20.pdf; JAIC Public Affairs, *JAIC Facilitates first-ever International AI Dialogue for Defense* (Sept. 16, 2020), https://www.ai.mil/news_09_16_20-jaic_facilitates_first-ever_international_ai_dialogue_for_defense_.html; Sydney J. Freedberg Jr., *Military AI Coalition of 13 Countries Meets on Ethics*, Breaking Defense (Sept. 16, 2020), https://breakingdefense.com/2020/09/13-nations-meet-on-ethics-for-military-ai/.

[599] AI Partnership for Defense, *Joint Statement* (Sept. 15-16, 2020), https://www.ai.mil/docs/AI_PfD_Joint_Statement_09_16_20.pdf.

[600] *Summary of the 2018 National Defense Strategy of the United States*, U.S. Department of Defense (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf; *National Security Strategy of the United States of America*, The White House (2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[601] Remarks by Stephen Biegun, Deputy Secretary of State, delivered at the U.S.-India Strategic Partnership Forum (Aug. 31, 2020), https://www.state.gov/deputy-secretary-biegun-remarks-at-the-u-s-india-strategic-partnership-forum/.

[602] *Secretary Pompeo's Quad Meeting with Japanese Foreign Minister Motegi, Indian Foreign Minister Jaishankar, and Australian Foreign Minister Payne*, U.S. Department of State, (Oct. 6, 2020), https://www.state.gov/secretary-pompeos-quad-meeting-with-japanese-foreign-minister-motegi-indian-foreign-minister-jaishankar-and-australian-foreign-minister-payne/; *The Second Japan-Australia-India-U.S. Foreign Ministers' Meeting*, Ministry of Foreign Affairs, Government of Japan (Oct. 6, 2020) https://www.mofa.go.jp/press/release/press6e_000244.html; *Australia-India-Japan-United States Quad Foreign Ministers' Meeting*, Minister for Foreign Affairs, Government of Australia (Oct. 6, 2020), https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-india-japan-united-states-quad-foreign-ministers-meeting; *2nd India-Australia-Japan-USA Ministerial Meeting*, Minister of External Affairs, Government of India (Oct. 6, 2020), https://www.mea.gov.in/press-releases.htm?dtl/33098/2nd+IndiaAustraliaJapan+USA+Ministerial+Meeting.

meeting built on a virtual meeting held on September 25, 2020, during which members reaffirmed their commitment to the rule of law and a few and open Indo-Pacific region.[603]

The Quad, and deepened cooperation in the Indo-Pacific, can be the foundation for a coordinated defense against potential hostile aggression from China and defense of shared interests, including a commitment to rules-based order.[604] Cooperation could take form, for example, in the annual Malabar naval exercise in the Bay of Bengal with broader participation from all Quad partners, other coordinated training and exercises, coordinated defense against information warfare, and intelligence sharing.

Proposed Executive Branch Action

The Commission encourages the Departments of State and Defense to build on the Quad framework and negotiate formal AI cooperation agreements in the Indo-Pacific region with Australia, India, and Japan, as well as with New Zealand, South Korea, and Vietnam. This could be done in connection with broader cooperation around conventional defense (and falling under existing defense cooperation agreements) or in a standalone manner, and could be undertaken bilaterally or multilaterally. In addition, development and application of AI and other emerging technologies should be a priority agenda item at both the ministerial and working level in order to achieve the interoperability required within defense partnerships.

Pillar II: Shaping Global AI Cooperation through Multilateral Forums

The growing ubiquity of AI and its increased global association with economic prosperity, security, and values has led to a proliferation of multilateral and international efforts intended to advance AI cooperation and address emerging challenges. These forums vary in their stakeholder composition, country membership, mandatory or obligatory nature, enforcement authority, and function (see Annex A).

This section begins with an assessment of promising multilateral efforts to develop AI norms and convene nations to address issues of AI development and use. It then addresses processes for developing international technical standards for AI.

Issue 1: Shaping the Global AI Terrain

Virtually every major international institution has launched a working group or policy initiative or endorsed a set of guiding principles or best practices for AI development and use. The Commission has assessed these efforts with particular attention to their overlap with U.S. national security interests and the promise they hold for constructive action in critical areas for global AI cooperation (see Pillar III).

[603] *Japan-Australia-India-U.S. Consultations*, Ministry of Foreign Affairs of Japan (Sept. 25, 2020), https://www.mofa.go.jp/press/release/press4e_002912.html; *India-Australia-Japan-United States Senior Officials Consultations*, Ministry of External Affairs, Government of India (Sept. 25, 2020), https://www.mea.gov.in/press-releases.htm?dtl/33059/IndiaAustraliaJapanUnited_States_Senior_Officials_Consultations; *U.S.-Australia-India-Japan Consultations ("The Quad")*, U.S. Department of State (Sept. 25, 2020), https://www.state.gov/u-s-australia-india-japan-consultations-the-quad-3/.

[604] Jeff Smith, *The Quad 2.0: A Foundation for a Free and Open Indo-Pacific*, Heritage Foundation (July 6, 2020), https://www.heritage.org/global-politics/report/the-quad-20-foundation-free-and-open-indo-pacific;

Organisation for Economic Co-operation and Development (OECD). The OECD has led the international community with its work around AI norms and associated policy development.[605] In May 2019, the United States and other nations adopted the OECD Principles on Artificial Intelligence as the first multilateral set of principles signed onto by governments.[606] These Principles, which the Department of State endorses, have been and will remain an important foundational document for further international work.[607]

2020 has witnessed a flourishing of multilateral initiatives to address the challenges and opportunities of AI and associated technologies. From a U.S. national security perspective, these are the most promising.

Global Partnership on Artificial Intelligence (GPAI). GPAI formally launched on June 15, 2020[608] to advance "responsible and human-centric" AI that is consistent with "human rights, fundamental freedoms," the founding country members' "shared democratic values," as well as "innovation and economic growth."[609] Led by France and Canada, GPAI's members, including the United States,[610] aim to bolster AI-related policies and priorities through technical expertise and targeted research. The United States Government, foreign governments, and civil society stakeholders have expressed optimism that GPAI will facilitate multi-stakeholder political and technical coordination across democracies.[611] The United States Government's decision to join the multi-stakeholder GPAI signaled to

[605] In 2016, its Committee on Digital Economy Policy (CDEP) began discussing the potential to use the OECD Council as an avenue to develop principles that fostered trust in AI and appointed an Expert Group on AI (AIGO) in 2018 to provide guidance on their development. *OECD Going Digital,* OECD (last accessed Sept. 16, 2020), https://www.oecd.org/going-digital/ai/; *OECD Creates Expert Group to Foster Trust in Artificial Intelligence,* OECD (Sept. 13, 2018), http://www.oecd.org/going-digital/ai/oecd-creates-expert-group-to-foster-trust-in-artificial-intelligence.htm.

[606] The principles were adopted by all 37 OECD members as well as Argentina, Brazil, Costa Rica, Malta, Peru, Romania, and Ukraine. *Recommendation of the Council on Artificial Intelligence,* OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Members of the G20, including China and Russia, endorsed the principles at the Osaka Summit in June 2019. See *G20 Ministerial Statement on Trade and Digital Economy*, https://www.mofa.go.jp/files/000486596.pdf.

[607] The OECD Network of Experts on AI (ONE AI) is an informal advisory group of 70 multi-disciplinary and multi-stakeholder experts and is chaired by a U.S. State Department official. Its memberships, from over 30 countries, provide policy, technical, and business expert input to inform OECD analysis and recommendations, particularly in its three working groups focused on classifying AI systems and providing implementation guidance on values-based AI principles and national AI policies. *OECD Network of Experts on AI (ONE AI),* OECD.AI (last accessed Sept. 16, 2020), https://oecd.ai/network-of-experts.

[608] Prior to the 2018 G7 Summit, France and Canada announced the creation of the International Panel on Artificial Intelligence (IPAI). France and Canada then announced the foundation of the Global Partnership on AI (GPAI) in August 2019 as well as the decision to support GPAI with two Centres of Expertise in October 2019. See *Launch of the Global Partnership on Artificial Intelligence by 15 Founding Members*, French Ministry for Europe and Foreign Affairs (June 15, 2020), https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/launch-of-the-global-partnership-on-artificial-intelligence-by-15-founding.

[609] *Joint Statement from Founding Members of the Global Partnership on Artificial Intelligence*, U.S. Department of State (June 15, 2020), https://www.state.gov/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence/.

[610] GPAI's membership includes Australia, Canada, France, Germany, India, Italy, Japan, Mexico, New Zealand, South Korea, Singapore, Slovenia, the United Kingdom, the United States, and the European Union with the OECD as a Permanent Observer. See *OECD to Host Secretariat of New Global Partnership on Artificial Intelligence*, OECD (June 15, 2020), https://www.oecd.org/going-digital/ai/oecd-to-host-secretariat-of-new-global-partnership-on-artificial-intelligence.htm.

[611] NSCAI staff interview with OpenAI (July 21, 2020); NSCAI staff interview with German Embassy (June 2, 2020); NSCAI staff interview with European Commission (June 15, 2020); see also *New Democratic Coalitions on 5G and AI Technologies,* LawFare (Aug. 6, 2020) https://www.lawfareblog.com/two-new-democratic-coalitions-5g-and-ai-technologies; *Microsoft Response to National Security Commission on Artificial Intelligence Request for Comments Re: Advancement of AI and Associated Technologies in the U.S.*, Docket No.: 05-2020-01, Microsoft (Sep. 28, 2020),

industry, technical experts, academia, allies and partners, and strategic competitors U.S. resolve about democratic coalition building to advance the development and use of AI.

OECD Policy Observatory (OECD.AI). In February 2020, the OECD launched OECD.AI, which aims to facilitate dialogue between its global stakeholders, provide evidence-based analysis on over 20 policy areas, promote the adoption of the OECD AI Principles, and bolster the advancement and monitoring of trustworthy AI systems that benefit society.[612]

D10. The United Kingdom (UK) proposed the coalition in March 2020 with a group of ten democratic nations—Australia, Canada, France, Germany, India, Italy, Japan, South Korea, the UK, and the United States.[613] Concerns about the Chinese government's handling of COVID-19, including its dissemination of faulty medical supplies, paired with growing international consensus that using Huawei's 5G infrastructure poses security and economic risks, prompted the UK to urge coordinated action to provide alternatives to Huawei and avenues for shifting global supply chains.[614] The initiative to gather this group of ten democracies has been applauded for building on the traditionally-used G7 to meet a challenge posed by great power competition in the digital age.[615] The UK's upcoming G7 Presidency may be used as a platform to strengthen an allied response to China.[616] As the D10 concept continues to develop and partners scope its mandate, D10 should consider supply chain security, interoperability, and the growing importance of SenseTime (in addition to Huawei). SenseTime, the largest algorithm provider and among the largest AI platforms in China, creates facial recognition software that is used by the Chinese government and by public and private entities worldwide.[617] Its clients included local police departments in the United States before the Department of Commerce placed SenseTime on the Entity List in October 2019 because of its role in human rights abuses in the autonomous region of Xinjiang.[618]

[612] *OECD.AI Policy Observatory*, OECD.AI (last accessed Sept. 16, 2020), https://www.oecd.org/going-digital/ai/about-the-oecd-ai-policy-observatory.pdf; *About OECD.AI,* OECD.AI (last accessed Sept. 16, 2020), https://oecd.ai/about; *Policy Areas Overview,* OECD.AI (last accessed Sept. 16, 2020), https://oecd.ai/policy-areas.

[613] *UK Seeks Alliance to Avoid Reliance on Chinese Tech: The Times,* Reuters (May 28, 2020), https://www.reuters.com/article/us-britain-tech-coalition/uk-seeks-alliance-to-avoid-reliance-on-chinese-tech-the-times-idU.S.KBN2343JW.

[614] Erik Brattberg & Ben Judah, *Forget the G-7, Build the D-10,* Foreign Policy (June 10, 2020), https://foreignpolicy.com/2020/06/10/g7-d10-democracy-trump-europe/; Bloomberg News, *How Huawei Landed at the Center of Global Tech Tussle: QuickTake,* The Washington Post (Aug. 19, 2020), https://www.washingtonpost.com/business/how-huawei-landed-at-the-center-of-global-tech-tussle-quicktake/2020/08/19/158cbc74-e1eb-11ea-82d8-5e55d47e90ca_story.html; Justin Sheman, *The UK is Forging A 5G Club of Democracies to Avoid Reliance on Huawei,* Atlantic Council (June 2, 2020), https://www.atlanticcouncil.org/blogs/new-atlanticist/the-uk-is-forging-a-5g-club-of-democracies-to-avoid-reliance-on-huawei/; Arindrajit Basu & Justin Sherman, *Two New Democratic Coalitions on 5G and AI Technologies*, Lawfare (Aug. 6, 2020), https://www.lawfareblog.com/two-new-democratic-coalitions-5g-and-ai-technologies.

[615] Edward Fishman & Siddharth Mohandes, *A Council of Democracies Can Save Multilateralism,* Foreign Affairs (Aug. 3, 2020), https://www.foreignaffairs.com/articles/asia/2020-08-03/council-democracies-can-save-multilateralism.

[616] Remarks by Baroness Helena Kennedy QC delivered at CSIS Online Event: Allied Cooperation on China (July 15, 2020), https://www.csis.org/events/online-event-allied-cooperation-china.

[617] Bernard Marr, *Meet the World's Most Valuable AI Startup: China's SenseTime*, *Forbes* (June 17, 2019), https://www.forbes.com/sites/bernardmarr/2019/06/17/meet-the-worlds-most-valuable-ai-startup-chinas-sensetime/#a0ab74309fcc.

[618] Lulu Yilun Chen, *Chinese AI Giant Blacklisted by Trump Thrives in Virus Era*, Bloomberg (Aug. 18, 2020), https://www.bloomberg.com/news/articles/2020-08-18/chinese-ai-giant-blacklisted-by-trump-mints-money-

Department of State Initiatives. In 2020, the Department of State launched a series of initiatives to build a coalition of trusted countries and companies to address various threats and challenges posed by emerging technologies, including and 5G and AI. These initiatives, such as the Clean Networks program, seek to build on shared trust principles and protect critical telecommunications and technology infrastructure, citizens' privacy, and intellectual property from malign actions undertaken by actors like the Chinese Communist Party.[619] The initiatives may prove successful vehicles to achieve cooperation on AI and associated technologies. Further clarity from the United States Government regarding the objectives and operations of these initiatives, as well as the participation of partner nations, is critical to develop these initiatives into one piece of a broader strategy to counterbalance China's Belt and Road Initiative and Digital Silk Road.

"T3." In September 2020, the United States, India, and Israel announced a new avenue in their partnership to "deliver the promise of 5G in a way that is open, interoperable, reliable, and secure." In the words of U.S. Agency for International Development Deputy Administrator Bonnie Glick, "We cannot allow any nation to dominate this technology or use it to dominate other nations."[620] The nascent partnership, described by experts as "T3", could serve as a model for other trilateral relationships around emerging technology or as a foundation for a larger coalition of nations with technological expertise and similar concerns about the threats around emerging technology.[621]

The Inter-Parliamentary Alliance on China (IPAC). IPAC launched in June 2020 to convene legislators from around the world to promote a multilateral policy position that develops trust and addresses economic, human rights-related, and technological challenges posed by China's shift in its domestic and international engagement. IPAC seeks to transcend political divisions with goals to safeguard the international legal order, uphold universal human rights, promote fair trade practices, and strengthen security and national integrity.[622] Membership includes two legislators of different political leanings from 17

from-virus; Ana Swanson and Paul Mozur, *U.S. Blacklists 28 Chinese Entities Over Abuses in Xinjiang*, The New York Times (Oct. 7, 2019), https://www.nytimes.com/2019/10/07/us/politics/us-to-blacklist-28-chinese-entities-over-abuses-in-xinjiang.html.

[619] For more information on these efforts see Michael Pompeo, *Announcing the Expansion of the Clean Network to Safeguard America's Assets*, U.S. Department of State (Aug. 5, 2020), https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/; *The Clean Network*, U.S. Department of State (last visited Sep. 29, 2020), https://www.state.gov/the-clean-network/; *Under Secretary Keith Krach Briefs the Press on Huawei and Clean Telcos*, U.S. Department of State (June 25, 2020), https://www.state.gov/telephonic-briefing-with-keith-krach-under-secretary-for-economic-growth-energy-and-the-environment/.

[620] Remarks by Bonnie Glick, Deputy Administrator of the U.S. Agency for International Development (USAID) delivered at the AJC Virtual Summit on U.S.-India-Israel Relations (Sept. 3, 2020), https://www.usaid.gov/news-information/speeches/sep-3-2020-da-glick-remarks-ajc-virtual-summit-us-india-israel.

[621] Gautam Chikermane, *From T3, the India-US-Israel Tech Alliance Can Become T11*, Observer Research Foundation (Sept. 10, 2020), https://www.orfonline.org/expert-speak/from-t3-the-india-us-israel-tech-alliance-can-become-t11-73161/.

[622] Baroness Helena Kennedy, Member of the UK House of Lords and member of the Labor Party, as well as Sir Iain Duncan Smith, previously UK Secretary of State for Work and Pensions and Leader of the Conservative Party, co-founded IPAC. Lady Kennedy has explained that despite different political beliefs, she and Sir Duncan Smith converge on the opinion that improved international coordination is needed to address challenges emanating from China. See Remarks by Baroness Helena Kennedy QC delivered at CSIS Online Event: Allied Cooperation on China (July 15, 2020), https://www.csis.org/events/online-event-allied-cooperation-china; see also *About*, Inter-Parliamentary Alliance on China (last accessed Sept. 16, 2020), https://www.ipac.global/about.

countries, who serve as national co-chairs, as well as other legislators—now numbering over one hundred—who support IPAC's mission statement.[623]

Figure 5.1 summarizes key multilateral AI initiatives across eight critical areas. **Annex A** contains further detail on each of these, along with a recommended prioritization for U.S. diplomatic and technical engagement.

Figure 5.1: Existing Multilateral AI Landscape

		DEFENSE & SECURITY	NORMS & STANDARDS	JOINT R&D	DATA-SHARING ECOSYSTEM	INNOVATION ENVIRONMENT	HUMAN CAPITAL	COUNTERING INFORMATION OPERATIONS	AI TO BENEFIT HUMANITY
COALITIONS FOCUSED ON AI & EMERGING TECHNOLOGY	D10 Initiative					X			
	Dept. of State Initiatives (e.g., Clean Networks)		X			X			X
	GPAI		X	X	X	X			
	IPAC		X			X			
	JAIC AI PfD	X	X	X	X				
	T3					X			
	TTCP AI Strategic Challenge	X		X					
INTERNATIONAL ORGANIZATIONS WITH AI-RELATED INITIATIVES	African Union (AU)		X		X				X
	Asia-Pacific Economic Cooperation (APEC)		X		X	X	X		
	Association of Southeast Asian Nations (ASEAN)		X			X			
	Council of Europe		X						X
	East Asian Summit (EAS)	X	X			X			
	G7	X	X	X	X	X		X	
	G20		X		X	X			
	NATO	X	X	X	X	X	X	X	
	Organization of American States (OAS)		X						X
	OECD + OECD.AI		X		X	X			
	OSCE		X						
	UNSG High-Level Panel on Digital Cooperation		X					X	X

[623] Co-chairs come from Australia, Canada, Czech Republic, Germany, European Parliament, France, Italy, Japan, Lithuania, the Netherlands, Norway, New Zealand, Switzerland, Sweden, Uganda, UK, and the U.S. See *Team*, Inter-Parliamentary Alliance on China (2020), https://www.ipac.global/team. Although IPAC has yet to pursue specific legislative efforts, its current "campaigns" address the intersection of undemocratic use of new technologies, human rights, and broader geopolitical concerns about China. In particular, IPAC has condemned China's use of surveillance in its persecution of the Uyghur people, which involves AI. The inclusion of countries across Europe as well as members from Japan and Uganda and a heavy U.S. representation, has led to optimism in the United States and abroad that IPAC—as the only international legislative effort of its kind—could be a valuable reinforcing mechanism for other efforts addressing great power competition in the digital age.

SPECIALIZED ORGANIZATIONS WITH AI-RELATED INITIATIVES	Freedom Online Coalition (FOC)		X					X	
	IEEE		X		X	X		X	
	IP5					X			
	ISO/IEC		X		X	X			
	ITU-T		X			X			X
	National Technology and Industry Base (NTIB)	X		X		X			
	UNESCO		X						X
	UN CCW GGE on LAWs	X	X						
	WIPO					X		X	
	WTO				X	X			

Recommendation 3: The United States, through the Department of State, should lead in developing the international AI environment by working with partners and adopting a "coalition of coalitions" approach to multilateral efforts.

While none of the many multilateral efforts around AI addresses all U.S. interests or all critical areas, many are promising. The Commission therefore recommends the Department of State adopt a "coalition of coalitions" approach to supplement traditional U.S. alliances: assessing the comparative strengths of each multilateral initiative, prioritizing those initiatives with the most potential that include the right groups of partners and allies, and using those forums to develop multilateral AI cooperation in new directions.

In addition to the benefits to be gained through the coalition efforts, this strategy will also help the United States to build goodwill by recognizing significant efforts already made by key partners and allies, avoid inevitable delays around creating new governance structures, and enable the United States Government to prioritize objectives and resources with key stakeholders.

To position itself best for success, the United States Government must define goals for each coalition, identify associated metrics of success, assign roles and responsibilities to government entities and individuals, and allocate resources. Critical to the success of this effort is the proposed role of the Technology Leadership Council, which would serve a necessary role in coordination, deconflicting, and priority setting for United States Government engagement, ensuring responsible offices are sufficiently staffed and resources and goals are met.[624]

Proposed Executive Branch Action

The United States Government, with the Department of State as lead—and coordinating through the proposed Technology Leadership Council—should:

[624] See Tab 4 of this report.

1. Continue to support OECD's international efforts and advance the implementation of the OECD AI Principles, as well as facilitate cooperation on developing a unified, allied position on addressing practices that undermine AI principles.

2. Foster emerging Department of State-led initiatives such as Clean Networks to develop a broad international coalition to align interests at the intersection of technology, innovation, and economics.

3. Engage proactively with France and Canada to help build GPAI into the premier multi-stakeholder forum to advance responsible AI and data governance, coordinate collaborative, multilateral R&D on AI and associated technologies, leverage AI for global needs such as pandemic response, and increase the U.S. role in providing research support to collaborative GPAI projects.

4. Engage closely with the UK to build the D10 initiative into a broader effort to counter Chinese efforts on technological innovation, using the 5G experience as a model to expand the coalition's program to other associated technologies.[625]

5. Develop a strategy for new initiatives focused on targeted, smaller groups of nations—using the U.S.-India-Israel "T3" as a model—to establish proofs of concept and explore collaborative approaches to AI and emerging technology before expanding to include more nations.

Recommendation 4: The President, through the Department of State, should initiate efforts to establish a Digital Coalition of democratic states and the private sector to coordinate efforts and strategy around AI and emerging technologies, beginning with a Digital Summit.

Multilateral efforts have flourished in the past year in part because democratic nations have realized how fundamental AI is to their economics and security and how they share common geopolitical threats, hope for the promise of technology, and concerns about its responsible development and application.

As the Commission has noted, there are many promising efforts in the international landscape. However, there is no forum for nations to convene government, civil society, and the private sector in order to address issues across the AI landscape—from new approaches to data sharing to collaborative R&D to defense applications to projects focused on global challenges like pandemics, disaster response, and climate change. Moreover, none of the

[625] "While there is no single, definitive list of which technologies are the most important, a general consensus is emerging in government around AI. The Commission examined five recent lists of emerging technologies critical to U.S. national security offered separately by DoD, the Department of Commerce, the President's Council of Advisors on Science and Technology, and in the Senate's Endless Frontier Act (S.3832) . . . Each list includes AI as a critical technology, while eight other technologies only appear in a majority of the lists: 1) biotechnology; 2) cybersecurity and data management; 3) quantum computing; 4) semiconductors; 5) robotics; 6) advanced communications; 7) advanced manufacturing; and, 8) Hypersonics." Joint Written Testimony of Dr. Eric Schmidt, Secretary Robert O. Work, Honorable Mignon Clyburn, and Dr. Jose-Marie Griffiths before the U.S. House of Representatives Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities, *Hearing on Interim Review of the National Security Commission on Artificial Intelligence Effort and Recommendations* at 1 (Sep. 17, 2020), https://www.congress.gov/116/meeting/house/110996/witnesses/HHRG-116-AS26-Wstate-SchmidtE-20200917.pdf.

existing forums has quite the right membership to consider a coordinated response of democratic nations to authoritarian regimes to strengthen a digital order reflecting democratic values.

Collaboration among democratic nations around development and use of AI and associated emerging technologies is now a strategic imperative to counter China's efforts and to realize the potential of AI to improve lives, grow innovative industries, empower workers, and increase national security.

The Commission believes the United States has the unique potential to lead an effort towards the creation of a Digital Coalition. The objectives of this Coalition will be to:

- Create a path forward for a democratic digital infrastructure with high standards for openness, security, and resiliency;
- Coordinate existing, overlapping multilateral efforts to enable participants to direct resources more efficiently;
- Convene private and public sector participants to pursue collaborative applications of AI and other emerging technologies to further the global economy, enhance international and national security, and address critical humanitarian needs;
- Develop and execute on a shared research agenda for strengthening key democratic advantages in digital technology;
- Coordinate the activities of democratic nations across the multiple standards setting bodies and multilateral organizations that shape the governance of emerging technologies;
- Expand and operationalize AI principles reflecting democratic values;
- Reconcile divergent views within democratic states about the employment of AI and other emerging technologies in domestic and international contexts; and
- Implement methods to safeguard democracies from malign use of emerging technologies.

Realizing these objectives through a Digital Coalition, however, must begin with a meeting of the minds of this diverse group of like-minded stakeholders. Therefore, the Commission proposes that the United States Government begin immediately to organize a Digital Summit in Washington, D.C.

Proposed Executive Branch Action

The President, through the Department of State, should convene a Digital Summit in Washington, D.C., to galvanize international coordination around AI and other emerging technologies. The Summit should include leaders and representatives from partner and ally nations, from the private sector, from civil society and academia, and from key international organizations. Organized around plenary sessions and working groups, the Summit, as envisioned, will seek to develop an overarching strategy for furthering shared interests and addressing common threats as well as concrete, operational plans to pursue international and cross-border collaboration around emerging technology.

Issue 2: Shaping International Technical AI Standards

China has, since at least 2015, reoriented its domestic standards process and implemented a concerted strategy to influence international standards setting.[626] The result has been an aggressive campaign to take an active role within international AI standards-setting organizations in order to advance its agenda.[627] Later this year, Beijing is expected to release "China Standards 2035," which should "provide a blueprint for how the Chinese government and leading Chinese companies can lead on and set standards related to a collection of key emerging technologies such as AI, 5G, and the Internet of Things"[628] and promote Chinese standards becoming the international norm through participation in standards bodies and encouraging adoption of Chinese standards through Belt and Road investments.[629]

China's top-down, state-led approach to standards-setting has enabled the government to employ a variety of tactics to shape international standards. China has invested heavily in R&D and programs aimed at strengthening technical talent necessary to develop technical standards.[630] China has also significantly increased its participation in each of the key standards development organizations (SDOs) for AI and associated technologies: the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Institute of Electrical and Electronic Engineers (IEEE), and the United Nations' International Telecommunication Union's Telecommunication Standardization Sector (ITU-T).[631] Likewise, the CCP encourages participants to volunteer for leadership

[626] "It is noteworthy that, in addition to vast internal consultations piloted by the State Council and the heads of relevant ministries, Beijing sought the counsel of high-level representatives from standards-coordinating bodies in the United States (ANSI), Germany (DIN), the UK (BSI), and France (AFNOR) in an effort to incorporate best practices." These consultations informed the 2017 Standardization Law. See John Seaman, *China and the New Geopolitics of Technical Standardization,* IFRI at 16 (Jan. 2020), https://www.ifri.org/sites/default/files/atoms/files/seaman_china_standardization_2020.pdf.

[627] John Seaman, *China and the New Geopolitics of Technical Standardization,* IFRI (Jan. 2020), https://www.ifri.org/sites/default/files/atoms/files/seaman_china_standardization_2020.pdf.

[628] See *Second Quarter Recommendations*, NSCAI at 81 (July 2020), https://www.nscai.gov/reports.

[629] Currently, China "has signed 85 standardization cooperation agreements with 49 countries and regions." *The BRI Progress, Contributions and Prospects,* China Daily (Apr. 23, 2019), http://chinadailyglobal.com/a/201904/23/WS5cbe5761a3104842260b7a41.html. If some countries opt for international standards and others utilize Chinese standards, there is a long-term fear of a bifurcation of technological spheres. See Jack Kamensky, *China's Participation in International Standards Setting: Benefits and Concerns for U.S. Industry,* China Business Review (Feb. 7, 2020), https://www.chinabusinessreview.com/chinas-participation-in-international-standards-setting-benefits-and-concerns-for-us-industry/; John Seaman, *China and the New Geopolitics of Technical Standardization,* IFRI (Jan. 2020), https://www.ifri.org/sites/default/files/atoms/files/seaman_china_standardization_2020.pdf.

[630] The Chinese Standardization Administration of China (SAC) seeks to have 60 "standards innovation bases" across China to improve China's standardization. See John Seaman, *China and the New Geopolitics of Technical Standardization*, IFRI at 12 (Jan. 2020), https://www.ifri.org/sites/default/files/atoms/files/seaman_china_standardization_2020.pdf; Translation of *Outline of the National Innovation-Driven Development Strategy Issued by the CPC Central Committee and the State Council,* Georgetown Center for Security and Emerging Technology (translated Dec. 11, 2019, published May 19, 2016), https://cset.georgetown.edu/wp-content/uploads/t0076_innovation_driven_development_strategy_EN.pdf.

[631] International technical AI standards are shaped primarily through four SDOs: The ISO and IEC, two private regulatory networks; the IEEE, a technical professional organization, through its Standards Association; and the ITU, a specialized UN agency, through its Telecommunication Standardization Sector (ITU-T). ISO and IEC

positions.[632] The result: between 2011 and 2020, China has increased its secretariat positions 73 percent at ISO and 67 percent at the IEC, while German and Japanese-held secretariat positions have remained flat and U.S.-held positions have dropped.[633]

Technical standards enable collaborative and force multiplying innovation and expand the interoperable marketplace. Standards increase trust through common foundations and frameworks that increase quality assurance, promote consumer safety, enable interoperability of products and services from different companies, facilitate consistent performance evaluations, and inform regulation.[634] SDOs have established consistent paper size formats, wireless network protocols, plugs for global electrical devices, and mobile communications networks.[635]

Standards also carry significant economic ramifications. Companies that align international standards with their technological specifications often benefit from first-mover advantages and path dependencies that facilitate market dominance and continued competitiveness.[636] Particularly common in the information and communications technologies sector, economic benefits for a specific company are magnified if it has patented a technology required by the standard as other companies subsequently must acquire that technology or product for compliance.[637] Conversely, the standard-essential patents (SEPs) can serve as a barrier to standards adoption or market competition as other companies may not be able to afford paying the royalties.[638]

created a joint committee focused on digital technologies in 1987 (JTC 1) and in 2017, jointly created Subcommittee 42 - Artificial Intelligence (JTC 1/SC 42) dedicated exclusively to AI Standards. See Peter Cihon, *Technical Report: Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development*, Future of Humanity Institute at the University of Oxford (Apr. 2019), https://www.fhi.ox.ac.uk/wp-content/uploads/Standards_-FHI-Technical-Report.pdf; *ISO/IEC JTC 1/SC 42,* ISO (last accessed Sept. 16, 2020), https://www.iso.org/committee/6794475.html.

[632] *China in International Standards Setting: USCBC Recommendations for Constructive Participation,* The U.S.-China Business Council (Feb. 2020), https://www.uschina.org/sites/default/files/china_in_international_standards_setting.pdf.

[633] Id. at 3.

[634] Jeffrey Ding, *Balancing Standards: U.S. and Chinese Strategies for Developing Technical Standards in AI,* The National Bureau of Asian Research (July 1, 2020), https://www.nbr.org/publication/balancing-standards-u-s-and-chinese-strategies-for-developing-technical-standards-in-ai/; *Standards & Measurements,* NIST (Mar. 23, 2020), https://www.nist.gov/services-resources/standards-and-measurements; Remarks by Peter Brown, European Parliament's Liaison Officer, delivered at Standards-Setting from a European Perspective Event from Center for Strategic and International Studies (Jul. 30, 2020), https://www.csis.org/events/online-event-standard-setting-european-perspective.

[635] Standards enable products to cross national borders, and as Hilary McGeachy, a fellow at the U.S. Studies Center in Sydney writes, provide "the connective tissue between technology and the market, providing specifications for products, services and systems." See Brad Glosserman, *Setting 'Simple' Standards is Critical Diplomacy,* Japan Times (Apr. 8, 2020), https://www.japantimes.co.jp/opinion/2020/04/08/commentary/japan-commentary/setting-simple-standards-critical-diplomacy/.

[636] John Seaman, *China and the New Geopolitics of Technical Standardization,* IFRI at 14 (Jan. 2020), https://www.ifri.org/sites/default/files/atoms/files/seaman_china_standardization_2020.pdf.

[637] These standard-essential patents (SEPs) can lead to billions in equipment sales and licensing royalties. Holding SEPs saves companies from sometimes exuberant "switching costs" to align their products with international standards and offers the potential to generate revenue from royalties. See *China in International Standards Setting: USCBC Recommendations for Constructive Participation,* The U.S.-China Business Council at 7 (Feb. 2020), https://www.uschina.org/sites/default/files/china_in_international_standards_setting.pdf; Bjorn Fagerster & Tim Ruhlig, *China's Standard Power and Its Geopolitical Implications for Europe*, Swedish Institute of International Affairs at 14 (Feb. 2019), https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2019/ui-brief-no.-2-2019.pdf.

[638] Given the potential negative impact of SEPs, standards bodies have developed different policies to prevent industry participants from 'capturing' a market. For example, the ISO requires participants disclose—as early as

Trade and companies' access to global markets is often conditioned on meeting standards of a particular country.[639] Increasing the utilization of international standards therefore lowers transaction costs for exporting industries.[640] Companies have indicated for many years that China uses additional domestic technical standards as a protectionist tool to impede trade, decrease international companies' access to the Chinese market, and protect their infant industries. A 2019 survey from the U.S.-China Business Council found 30 percent of member companies reporting standards-related protectionism in China.[641]

The United States Government has recognized that technical standards, particularly international standards, are integral to protecting U.S. national security, values, and economic prosperity.[642] The National Artificial Intelligence Research and Development Strategic Plan classifies AI standards and benchmarks as a research priority for U.S. departments and agencies.[643] In February 2019, the President issued Executive Order (E.O.) 13859, including "development of appropriate technical standards" as one of the five principles to guide the American AI Initiative. The E.O. instructed U.S. departments and agencies to "develop international standards to promote and protect" innovation as well as public trust and confidence in AI. E.O. 13859 also directed the Secretary of Commerce,

possible during the standards development process—whether they have a patent or pending patent application for a covered technology. After disclosure, participants must state whether they are willing to negotiate providing licenses required by the patent to other companies free of charge and/or on reasonable and non-discriminatory terms. See Robynne Sanders, et al., *The Ongoing Problem with Standards and Patents,* DLA Piper (2017), https://www.dlapiper.com/en/global/insights/publications/2017/12/ipt-news-asia-pacific-december-2017/the-ongoing-problem-with-standards-and-patents/.

[639] The linkage between trade and standards is compounded by the WTO's formal treatment of ISO and IEC technical standards as references, which further diffuses international standards adoption. Additionally, the WTO's Agreement on Technical Barriers to Trade (TBT)—which China is a signatory to—stipulates that countries use international standards, where they exist, and prohibits the use of additional domestic standards as a protectionist tool to impede trade. See John Seaman, *China and the New Geopolitics of Technical Standardization,* IFRI at 13 (Jan. 2020), https://www.ifri.org/sites/default/files/atoms/files/seaman_china_standardization_2020.pdf; *Agreement on Technical Barriers to Trade*, World Trade Organization, https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm#annexIII.

[640] Because countries' adoption of international standards is voluntary, the United States and likeminded allies, particularly in Europe, have for many years urged countries like China to increase their participation in international standards bodies. The goals of this heightened inclusivity included constructive and unbiased participation that caused expanded standards compatibility, international standards adoption, and opportunities for technical discussions in neutral forums. See Bjorn Fagerster & Tim Ruhlig, *China's Standard Power and Its Geopolitical Implications for Europe,* Swedish Institute of International Affairs (Feb. 2019), https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2019/ui-brief-no.-2-2019.pdf; John Seaman, *China and the New Geopolitics of Technical Standardization,* IFRI (Jan. 2020), https://www.ifri.org/sites/default/files/atoms/files/seaman_china_standardization_2020.pdf; *China in International Standards Setting: USCBC Recommendations for Constructive Participation,* The US-China Business Council at 3-4 (Feb. 2020), https://www.uschina.org/sites/default/files/china_in_international_standards_setting.pdf; NSCAI staff discussions with industry representatives (Aug. 28, 2020, Sept. 3, 2020).

[641] Bjorn Fagerster &Tim Ruhlig, *China's Standard Power and Its Geopolitical Implications for Europe,* Swedish Institute of International Affairs (Feb. 2019), https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2019/ui-brief-no.-2-2019.pdf; Jack Kamensky, *Standards Setting in China: Challenges and Best Practices,* The US-China Business Council at 11 (Feb. 2020), https://www.uschina.org/sites/default/files/standards_setting_in_china_challenges_and_best_practices.pdf.

[642] Arjun Kharpal, *U.S. Firms Can Work with Huawei on 5G and Other Standards. Here's What it Means,* CNBC Markets (June 15, 2020), https://www.cnbc.com/2020/06/16/us-firms-can-work-with-huawei-on-5g-and-other-standards.html.

[643] AI standards were classified as a research priority in both the 2016 Strategic Plan and the 2019 Update to the Strategic Plan. See *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update,* National Science and Technology Council (June 2019), https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf; *The National Artificial Intelligence Research and Development Strategic Plan,* National Science and Technology Council (Oct. 2016), https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf.

through the National Institute of Standards and Technology (NIST), to issue "a plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies."[644] NIST's subsequent report focused on a number of AI standards focus areas, both technical and non-technical.[645] Its corresponding recommendations included actions such as designating a Standards Coordinator to increase alignment and cooperation with other Federal agencies, increasing staff participation in standards development through training and adequate career development and promotions, promoting research to facilitate standards development, expanding public-private partnerships, and engaging internationally "to advance AI standards for U.S. economic and national security needs."[646]

Despite these actions, the U.S. national standards-setting process, as well as U.S. participation in international standards setting bodies, is still led by U.S. industry.[647] The United States Government and industry widely viewed standardization as non-political because the voluntary consensus-driven approach relied on technical expertise, research, and robust procedures.[648] The United States strongly believes that standards bodies should remain apolitical and free from nation state bias or favoritism.

Given the importance of AI standards and the concerning behaviors undertaken by China—and increasingly by other standards newcomers that are aligning with China and copying their strategy[649]—the United States Government must take steps internally to champion international technical standards that promote and protect U.S. interests related to AI, data, and associated technologies and infrastructure, and to reaffirm a commitment to the neutrality of SDOs.

Although U.S. departments and agencies—as consumers of standardized products and services—are heavily impacted by the output of the process, the United States Government's primary strategy is "private sector leadership, supplemented by Federal Government contributions to discrete standardization processes."[650] American National Standards

[644] Donald J. Trump, *Executive Order on Maintaining American Leadership in Artificial Intelligence,* The White House (Feb. 11, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

[645] See *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*, NIST (Aug. 9, 2019), https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

[646] Id.

[647] *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*, NIST (Aug. 9, 2019), https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf; Jack Kamensky, *Standards Setting in China: Challenges and Best Practices,* The US-China Business Council (Jan. 2020), https://www.uschina.org/sites/default/files/standards_setting_in_china_challenges_and_best_practices.pdf.

[648] Bjorn Fagerster & Tim Ruhlig, *China's Standard Power and Its Geopolitical Implications for Europe,* Swedish Institute of International Affairs (Feb. 2019), https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2019/ui-brief-no.-2-2019.pdf; John Mitchell, *The World Needs American Leadership in Setting the Technological Standards of the Future,* Nextgov (Aug. 31, 2020), https://www.nextgov.com/ideas/2020/08/world-needs-american-leadership-setting-technological-standards-future/168011/; NSCAI staff interview with Microsoft (Aug. 28, 2020).

[649] NSCAI staff interview with industry representatives (Aug. 12, 2020).

[650] Dong Geun Choi & Erik Puskar, *A Review of U.S.A. Participation in ISO and IEC,* NIST at ii (June 2014), https://www.nist.gov/system/files/nistir_8007-reviewofusparticip_isoiec-2014_0.pdf; *ITI Response to NIST-2019-0001 on Artificial Intelligence Standards,* Information Technology Industry Council (ITI) at 2 (Jun. 5, 2019), https://www.nist.gov/system/files/documents/2019/06/06/nist-ai-rfi-informatio-_technolog-_industry-council-001.pdf.

Institute (ANSI)[651] and NIST[652] support the advancement of U.S. standardization interests globally.

International standardization of AI and associated technologies has revealed the asymmetries between the Chinese government-led and U.S. industry-led approaches to SDOs, prompting a reevaluation of the current posture of the United States Government and industry towards standards-setting to protect and promote U.S. interests. Proactive participation in international standards bodies requires significant budget, personnel, and time commitments, and leadership roles—such as editorships—demand consistent engagement, sometimes for years. Larger companies are more likely to participate in the voluntary process given the expenses associated with funding devoted personnel and travel to international meeting locations.[653] Furthermore, as NIST recognizes, timing is critical: premature standards may impede innovation as technology continues to develop, while too-late efforts may deliver standards that do not match the built-up infrastructure.[654] Partnership and information-sharing between the United States Government and industry is therefore critical[655] to ensure protection of national security concerns involving standards.

United States Government-led dialogue with U.S. industry, as well as democratic allies, can help overcome information asymmetries and confusion over interests that hinder the advancement of AI technical standards that foster economic growth and protect consumers.[656]

[651] For example, ANSI, as the sole U.S. representative to ISO, accredits a U.S. Technical Advisory Group (U.S. TAG) to the ISO to "develop and transmit, via ANSI, U.S. positions on activities and ballots of the Technical Committees (and as appropriate, Subcommittees and policy committees)." United States Government departments and agencies can serve as members of the TAGs. See *ANSI Accredited U.S. Technical Advisory Groups (TAGs) to ISO,* ANSI (last accessed Sept. 16, 2020), https://www.ansi.org/standards_activities/iso_programs/tag_iso.

[652] The U.S. Federal Government—led by NIST's Standards Coordination Office—provides technical expertise to the development of standards, contributes personnel to the standards meetings and advisory groups, incorporates voluntary standards into U.S. regulations, and provides industry requirements to related standards projects. The relationship between ANSI and NIST is governed by a Memorandum of Understanding providing for the two bodies to cooperate in linking private sector and government interests, enhance and strengthen national voluntary consensus standards, and support U.S. competitiveness and economic growth. *ANSI Accredited U.S. Technical Advisory Groups (TAGs) to ISO,* ANSI (last accessed Sept. 16, 2020), https://www.ansi.org/standards_activities/iso_programs/tag_iso; *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*, NIST (Aug. 9, 2019), https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

[653] NSCAI staff interviews with technology industry representatives (Aug. 28, 2020; Sept. 3, 2020); Dong Geun Choi & Erik Puskar, *A Review of U.S.A. Participation in ISO and IEC,* NIST at 1 (June 2014), https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8007.pdf; *China in International Standards Setting: USCBC Recommendations for Constructive Participation,* The US-China Business Council at 9 (Feb. 2020), https://www.uschina.org/sites/default/files/china_in_international_standards_setting.pdf; Charles Schmidt, *Best Practices for Technical Standard Creation,* MITRE at 30 (Apr. 2017), https://www.mitre.org/sites/default/files/publications/17-1332-best-practices-for-technical-standard-creation.pdf.

[654] See *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*, NIST at 9 (Aug. 9, 2019), https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

[655] "With respect to standardization in Artificial Intelligence (AI), it is important that U.S. industry and the United States Government see each other as essential partners." *Response to Draft "Plan for Federal Engagement in Developing Technical Standards and Related Tools,"* Information Technology Council (ITI) (July 19, 2020), https://www.nist.gov/system/files/documents/2019/09/16/iti-comments-07192019.pdf.

[656] In a joint statement following a 2018 meeting of then-EC President Jean-Claude Juncker to the United States, the United States and the EU highlighted the importance of alignment on technical standards, particularly to facilitate trade, cut costs, and decrease bureaucratic obstacles. The joint statement urged a close dialogue and improved coordination to improve "cooperation and coordination with the U.S. in the framework of

Recommendation 5: The President should issue an E.O. to prioritize United States Government-efforts around technical standards through improved interagency coordination and improved collaboration with U.S. industry.

While E.O. 13859, issued in February 2019, provided a solid foundation for the United States Government to organize around the importance of technical standards in AI development, there remains a need to better coordinate United States Government positions—especially on national security—and enhance the mechanisms for ensuring those interests are conveyed in SDO deliberations. To achieve these goals, the Commission recommends that the President issue an E.O. re-emphasizing the critical importance of international technical standards, creating a framework for interagency coordination, and establishing a task force for promoting collaboration between the United States Government and industry officials.

First, the E.O. should create an interagency coordination task force for sharing threat information and identifying U.S. national security interests related to technical standards. This is consistent with the NIST report issued pursuant to E.O. 13859. The task force would include United States Government officials focused on U.S. national security from the Departments of State, Defense, Energy, Commerce, and Homeland Security as well as officials from the entire United States Intelligence Community. This could be modeled after the Office of Science and Technology Policy's (OSTP) Joint Committee on Research Environments (JCORE), the Department of State's International Digital Economy and Telecommunication Advisory Committee (IDET), the National Science Technology Council's Machine Learning and Artificial Intelligence Subcommittee, the Network and Information Technology Research and Development program's AI R&D Interagency Working Group, and the DoD's Artificial Intelligence Working Group but with an explicit focus on standardization and a broader lens to capture national security concerns across the range of United States Government interests.[657] The task force would be directed to prioritize issues, drive consensus, and implement community-based AI standards that could then be incorporated into the international SDO processes.

Second, the E.O. should direct the interagency task force to improve collaboration and partnership with industry, which is critical because industry organizations have a lead role in SDO efforts. The task force should explore formalizing a government-industry forum to improve government communication of national security interests and discuss actions, as needed, to address SDO deliberative and governance issues. The Commission's discussions

international standard setting bodies." See *Progress Report on the Implementation of the EU-U.S. Joint Statement on 25 July 2018*, European Commission at 6 (2019), https://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158272.pdf.

[657] More information on these groups can be found at: *Summary of the 2019 White House Summit of the Joint Committee on the Research Environment (JCORE),* Executive Office of the President of the United States (Nov. 2019), https://www.whitehouse.gov/wp-content/uploads/2019/11/Summary-of-JCORE-Summit-November-2019.pdf; *Charter of the United States International Digital Economy and Telecommunication Advisory Committee,* U.S. Department of State (June 30, 2020), https://www.state.gov/charter-of-the-united-states-international-digital-economy-and-telecommunication-advisory-committee/; *Charter of the Subcommittee on Machine Learning and Artificial Intelligence, Committee on Technology, National Science and Technology Council,* Executive Office of the President of the United States (May 6, 2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/ostp/MLAI_Charter.pdf; *Artificial Intelligence Interagency Working Group,* NITRD (last accessed Sept. 17, 2020), https://www.nitrd.gov/nitrdgroups/index.php?title=AI.

with industry representatives have recommended improved coordination so long as it preserves the U.S. approach for industry-led standards setting, which this Commission endorses. Appropriate SDOs for engagement would be determined by NIST,[658]including industry technical advisory groups (TAGs) like the ANSI InterNational Committee for Information Technology Standards (INCITS)/AI,[659] which serves as the U.S. TAG[660] for SC 42.[661]

Third, the E.O. should direct agencies mentioned above to resource and support regular and active participation by the United States Government in international standards-setting activities.[662] Subject matter experts from across the interagency should be encouraged to support and conduct research designed to guide development of AI standards positions. They must also have adequate funding to attend meetings and pursue career development opportunities in this rapidly changing field. In addition, U.S. officials must be able to devote the requisite time and resources associated with international standards setting and relevant government experts should be empowered—and encouraged—to volunteer for leadership positions, like editorships, through support and sufficient funding from their departments and agencies. Increased government attendance will help provide diplomatic expertise to U.S. delegations. The Department of State should also explore ways to provide diplomatic training of technical and subject matter experts (government and industry participants).

Fourth, the E.O. should direct NIST, through the Director of NIST and the Standards Coordinator, to collaborate with the private sector to create an industry-funded Standardization Center to share best practices and other information towards the development of standards.[663] Modeled on the Information Sharing and Analysis Center, which was created by the private sector in 2000 to share information on cybersecurity threats and vulnerabilities, the Standardization Center, as a public-private partnership, would

[658] See *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*, NIST (Aug. 9, 2019), https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

[659] The InterNational Committee for Information Technology Standards (INCITS) is a forum for developing standards among U.S. companies. INCITS serves as the technical advisory group for SC 42. See *INCITS Annual Report,* INCITS (last accessed Oct. 1, 2020), https://www.incits.org/symposium/annual-report/INCITS-AI.pdf.

[660] "The primary purpose of U.S. TAGs is to develop and transmit, via ANSI, U.S. consensus positions and comments on activities and ballots of ISO TCs (and, as appropriate, SCs, PCs, and policy committees)." See *ANSI-Accredited U.S. Technical Advisory Groups (TAGS) to ISO,* ANSI (last accessed Oct. 1, 2020), https://www.ansi.org/iso/ansi-activities/us-tags.

[661] SC42 (Artificial Intelligence) under ISO/IEC JTC 1 "is the primary standards development technical committee in which foundational AI standards are being developed." *ITI Response to NIST-2019-0001 on Artificial Intelligence Standards,* Information Technology Industry Council (ITI) (Jun. 5, 2019), https://www.nist.gov/system/files/documents/2019/06/06/nist-ai-rfi-informatio-_technolog-_industry-council-001.pdf.

[662] The Information Technology Industry Council (ITI), for example, has described the United States government as "too often limited in their ability to provide input due to budgetary resource constraints" and expressed support for alignment of Federal Government requirements and "a coordinated, shared representation of the totality of U.S. Federal Government AI expert participation" will help "maximize exposure while minimizing resource requirements" of the Federal Government. *Response to Draft "Plan for Federal Engagement in Developing Technical Standards and Related Tools,"* ITI Council (July 19, 2020), https://www.nist.gov/system/files/documents/2019/09/16/iti-comments-07192019.pdf.

[663] For example, "NIST can leverage its research into measurement (among other issues), which will be important to international standards work focusing on computational aspects of AI such as benchmarking. NIST research around tools to assess standard data sets would also help increase interoperability and access to data for AI." *ITI Response to NIST-2019-0001 on Artificial Intelligence Standards,* ITI Council (June 5, 2019), https://www.nist.gov/system/files/documents/2019/06/06/nist-ai-rfi-informatio-_technolog-_industry-council-001.pdf.

improve industry coordination and improve the U.S. industry's position in SDO proceedings.[664] The Standardization Center will also facilitate coordination of supporting and conducting research and evaluation necessary for technical standards development.

Proposed Executive Branch Action

The President should issue an E.O. to: (a) create an interagency coordination task force for sharing threat information and identifying U.S. national security interests related to AI technical standards; (b) direct the interagency task force to improve partnership and collaboration with industry; (c) direct federal agencies to resource and support focused research and evaluation and regular and active participation by the United States Government in international standards-setting activities; and (d) require the Director of NIST and the Standards Coordinator to encourage the private sector to create a Standardization Center to improve sharing of best practices and other information relevant to standards development, as well as support focused research coordination.

Recommendation 6: Congress should appropriate funds to NIST and key agencies for a dedicated interagency AI standards team to support the U.S. AI Standards Coordinator.

NIST is the main coordinator between government and industry on technical AI standards. NIST would strategically benefit from funding to devote the resources NSCAI has assessed as necessary to facilitate coordination with U.S. industry, the interagency, and democratic nations. At a minimum, Congress should appropriate funds sufficient to support at least 5 full-time equivalent personnel at NIST and at least one full-time equivalent each at the Departments of State, Defense, Homeland Security, and Energy and the Office of the Director of National Intelligence, and other agencies as may be appropriate. These personnel would, in addition to supporting focused research and undertaking other responsibilities necessary for technical standardization, participate in SDOs in order to bring their unique and critical perspectives to bear on U.S. standards development efforts.

Proposed Legislative Branch Action

Congress should appropriate funds sufficient to support at least ten full-time equivalent personnel to coordinate United States Government efforts in the development of international standards around AI, with funds supporting salaries and expenses associated with standardization research and development efforts as well as attendance at SDO meetings.

Recommendation 7: Congress should establish a Small Business Administration grant program to enable small- and medium-sized U.S. AI companies to participate in international standardization efforts.

Congress should authorize a grant program for small- and medium-sized U.S. AI companies to cover the high costs of engaging in international standardization efforts, including

[664] PDD/NSC 63 led to the creation of the Information Sharing and Analysis Center (ISAC). See Bill Clinton, *Presidential Decision Directive/NSC-63*, The White House (May 22, 1988), https://fas.org/irp/offdocs/pdd/pdd-63.htm.

conducting relevant research, developing requisite skills and expertise, preparing standards proposals, and attending SDO meetings. Their input enables greater technological innovation, helps prevent potential high "switching costs" that may impede their growth, and facilitates solution development for standards that impede exporting by these small businesses. The Commission proposes that Congress appropriate an initial amount of $1 million to fund grants issued by the Small Business Administration (SBA). In evaluating grant applications and awarding grants, SBA shall coordinate with the Director of NIST.

Proposed Legislative Branch Action

Congress should create a grant program as outlined above and appropriate $1 million annually to support grants to small- and medium-sized U.S. AI companies.

Recommendation 8: Under NIST's lead, the United States Government, in coordination with U.S. industry as well as U.S. allies, should promote international standardization in areas that further U.S. and allies' national security and defense interests in the appropriate and responsible use of AI.

The United States Government and relevant TAGs or parties responsible for developing, transmitting, and representing U.S. consensus positions at SDOs, must ensure U.S. national security and defense interests are considered and prioritized. It is the Government's responsibility to ensure that organizations representing the United States at SDOs, such as INCITS/AI, are aware of these interests and that necessary officials from NIST, Department of State, and other agencies engage as necessary in SDO meetings.

To develop national security-informed positions on technical AI standards, the Government must prioritize its underlying research. As it does so, NIST and other agencies should consider the Commission's *Key Considerations for Responsible Development and Fielding of AI*.[665] Among the *Key Considerations* relevant to U.S. national security and defense interests are technical standards for: (a) safety and reliability; (b) privacy-enhancing technologies, including PPML, cryptographic code, and other privacy-enhancing technologies; (c) data sharing, labelling, and related documentation for data, models and systems; (d) assessing system performance per shared values (including fairness, interpretability, reliability, and robustness); (e) traceability, focused on audit trail requirements per mission needs for high-stakes AI systems including safety-critical applications; and (f) interoperability including benchmarks that assess reliability of produced model explanations.

The United States Government, led by the Department of State, should engage with democratic nations to align positions on standards that are critical to mutual security and defense. This should be done in coordination with NIST, which has responsibility for developing U.S. positions on the technical and scientific aspects of international standards. The Department of State, as recommended in the quarter two report, is in the process of placing technology officers in major foreign technology hubs. This development will facilitate diplomatic efforts towards coordinating positions with allies and partners.

[665] See *Key Considerations.*

Proposed Executive Branch Action

NIST should coordinate United States Government positions on national security and defense interests to ensure those positions are reflected by TAGS, including INCITS/AI. NIST should consider the Commission's *Key Considerations* in prioritizing areas for standardization.

Pillar III: Building Resilient Bilateral AI Cooperation with Key Allies and Partners

The United States must deepen AI cooperation and strengthen the resiliency of U.S. alliances and partnerships to prevail against the challenges posed by great power competitors.[666] While the challenges are global in nature, the Indo-Pacific and Transatlantic regions in particular face new threats which we must meet together, based on shared values and tangible ways to prevail over undemocratic alternatives. AI will provide capabilities to identify those challenges and opportunities that will allow us to respond to such conditions faster and more effectively.

The United States should adopt a multi-faceted strategy to marshal global AI cooperation to advance a front of free, open, and innovative societies around shared defense and security needs, developing AI standards and norms, fostering joint R&D, improving data sharing capabilities, promoting innovation, fostering technical expertise, countering disinformation, and advancing AI applications to benefit humanity. The Commission proposes a *Blueprint for AI Cooperation*—concrete, operational projects, applications, and implementation methods in each of these eight critical areas for the United States to explore with a group of key allies and partners.

Issue 1: Allies and Partners for AI Cooperation

Recommendation 9: The United States should center its Indo-Pacific relationships around India including by creating a U.S.-India Strategic Tech-Alliance.

The Commission recommends that the United States prioritize efforts to solidify and further relationships with India. The United States and India have a longstanding relationship and the geopolitical importance of India as the world's largest democracy and second most populous country cannot be underestimated.

The partnership between the two nations, as the Department of State describes it, "is founded on a shared commitment to freedom, democratic principles, equal treatment of all citizens, human rights, and the rule of law" and spans shared interests including "promoting global security, stability, and economic prosperity through trade, investment, and

[666] The importance of strengthening partnerships in the Indo-Pacific region continues to grow as Russia and China increase their own collaborative work around advanced technology. See Samuel Bendett & Elsa Kania, *The Resilience of Sino-Russian High-Tech Cooperation*, War on the Rocks (Aug. 12, 2020), https://warontherocks.com/2020/08/the-resilience-of-sino-russian-high-tech-cooperation/; see also Andrea Kendall-Taylor & Jeffrey Edmonds, *Addressing Deepening Russia-China Relations*, CNAS (Aug. 31, 2020), https://www.cnas.org/publications/commentary/addressing-deepening-russia-china-relations.

connectivity."[667] India is considered a Major Defense Partner of the United States and the nations have deepened their cooperation through the U.S.-India 2+2 Ministerial Dialogue, begun in 2018, which includes the U.S. Secretaries of State and Defense and the Indian Ministers of External Affairs and Defence, and the U.S.-India Comprehensive Global Strategic Partnership, launched in February 2020.[668]

The United States and India already have a strong science and technology (S&T) relationship, reflected in the nations' Indo-U.S. Science and Technology Forum (IUSSTF), established in 2000; the 2005 S&T Cooperation Agreement, the annual U.S.-India Cyber Dialogue; and the U.S.-India Information and Communication Technology Working Group.[669]

In recent years, India has redoubled its efforts to improve its AI infrastructure (including through key investments by U.S. organizations[670]), faces immediate threats to its territorial and cyberspace integrity from China,[671] and has been an active participant in the most promising new multilateral efforts around AI such as GPAI and is part of the emerging D10 coalition. India boasts domestic technological expertise unlike any other and its citizens represent over 70 percent of the H-1B visas issued annually by the United States.[672]

Alignment between the two nations is clear and the potential to build on an already strong relationship is enormous.

[667] *U.S. Relations with India: Bilateral Relations Fact Sheet*, U.S. Department of State (July 28, 2020), https://www.state.gov/u-s-relations-with-india/.

[668] Media Note, U.S. Department of State, Intersessional Meeting of the U.S.-India 2+2 Ministerial Dialogue (September 11, 2020), https://www.state.gov/intersessional-meeting-of-the-u-s-india-22-ministerial-dialogue/; *Joint Statement: Vision and Principles for the United States-India Comprehensive Global Strategic Partnership*, The White House, (Feb. 25, 2020), https://www.whitehouse.gov/briefings-statements/joint-statement-vision-principles-united-states-india-comprehensive-global-strategic-partnership/.

[669]*About Us*, Indo-U.S. Science and Technology Forum (last accessed Sept. 16, 2020), https://iusstf.org/about-iusstf; *United States and India Sign Science and Technology Cooperation Agreement*, U.S. Department of State (Oct. 17, 2005), https://2001-2009.state.gov/r/pa/prs/ps/2005/55198.htm; *Joint Statement: 2016 United States-India Cyber Dialogue*, The White House (Sept. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/09/29/joint-statement-2016-united-states-india-cyber-dialogue; *Joint Statement from the U.S.-India Information Communications Technology Working Group*, US Mission India (Sept. 29, 2016), https://in.usembassy.gov/joint-statement-u-s-india-information-communications-technology-working-group.

[670] See, e.g., Andrew Trsiter, *Code vs. COVID-19,* Bill & Melinda Gates Foundation (2020), https://www.gatesfoundation.org/TheOptimist/Articles/coronavirus-andrew-trister-data-science. Google recently announced it will be launching an AI research lab in Bengaluru which will be led by Manish Gupta, a fellow from Society for Experimental Mechanics, and Milind Tambe, Director of the Harvard Center for Computation & Society. See Anam Ajmal, *Google Launches Artificial Intelligence Research Lab in Bengaluru,* Times of India (Sept. 19, 2019), https://timesofindia.indiatimes.com/business/india-business/google-launches-artificial-intelligence-research-lab-in-bengaluru/articleshow/71203154.cms.

[671] C. Raja Mohan, *Today, India's Strategic Autonomy is about Coping with Beijing's Challenge to its Territorial Integrity, Sovereignty,* News Bundle Online (Aug. 25, 2020), https://newsbundleonline.com/today-indias-strategic-autonomy-is-about-coping-with-beijings-challenge-to-its-territorial-integrity-sovereignty/; C. Raja Mohan, *Global Coalition of Democracies, Amid China's Assertion, Could Open a Range of New Possibilities,* The Indian Express (July 28, 2020), https://indianexpress.com/article/opinion/columns/us-india-democracy-china-cold-war-global-economy-6526409/; Arjun Kharpal, '*Chinese Firms are Learning a Painful Lesson': India's App Crackdown Opens Doors for U.S. Tech Giants,* CNBC (Sept. 4, 2020), https://www.cnbc.com/2020/09/04/india-crackdown-on-chinese-tech-opens-doors-for-us-giants.html.

[672] *Characteristics of H-1B Specialty Occupation Workers - Fiscal Year 2019 Annual Report to Congress*, U.S. Citizenship and Immigration Services at 6, 8 (Mar. 5, 2020), https://www.uscis.gov/sites/default/files/document/reports/Characteristics_of_Specialty_Occupation_Workers_H-1B_Fiscal_Year_2019.pdf.

To implement a more robust policy towards India, the Department of State, in coordination with the Departments of Defense and Commerce, must lead the creation of a U.S.-India Strategic Tech Alliance (UISTA). The objective of UISTA will be to make India a focal point of U.S. foreign policy in the region and an overarching Indo-Pacific strategy focused on emerging technology and India's increasingly important geopolitical role. The nations should engage in periodic high-level meetings to develop overarching strategy on issues involving emerging technology and the Indo-Pacific region. Through regular working groups, UISTA should develop and implement concrete, operational avenues for cooperation between the two nations—including advanced joint research and development projects around AI; talent exchanges and talent flow; a range of issues on innovation, including emerging technology investment and aligning export controls, investment screening, and intellectual property rights; development of AI for societal applications; and using AI to counter disinformation.

Proposed Executive Branch Action

The Department of State, in partnership with the India's Ministry of External Affairs, should establish UISTA to develop and implement strategy for emerging technology and the Indo-Pacific region. The nations should use an inaugural high-level meeting to develop an overarching strategy for the partnership and identify an agenda for concrete action to be pursued through working group meetings. Participation from the United States Government should also include the Departments of Defense, Energy, and Commerce.

Recommendation 10: The Department of State should create a Strategic Dialogue for Emerging Technologies with the European Union (EU).

The United States must also strengthen the resiliency of its Transatlantic alliances and partnerships around AI and emerging technologies, beginning with the EU. The EU and its 27 member states are among the United States' most important political, diplomatic, and commercial partners. The United States and the EU are the world's largest economies and trading partners and have, historically, pursued significant collaboration on science and technology.[673]

The EU approach to AI recognizes its strategic importance and addresses "technological, ethical, legal and socio-economic aspects to boost EU's research and industrial capacity and to put AI at the service of European citizens and economy."[674] Complementing the AI strategy is the EU's overarching goals to achieve technological sovereignty, with control over

[673] The United States and EU leverage the *Agreement for Scientific and Technological Cooperation between the European Community and the Government of the United States of America* which has been extended every five years since it came into force in 1998. They also collaborate through the Joint Consultative Group, the EU-US Space Dialogue, the Transatlantic Ocean Research Alliance, the Energy Council and the Transatlantic Economic Council. See *Scientific and Technological Cooperation Between the EU and the United States*, EUR-Lex (May 20, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ari0009; *Roadmap for EU-USA S&T Cooperation*, European Commission (Oct. 2017), https://ec.europa.eu/research/iscp/pdf/policy/us%20clean_roadmap_2017.pdf; see also Richard L. Hudson, *Tale of Two Cities: Brussels and Washington Struggle to Cooperate in Science,* Science Business (May 14, 2018), https://sciencebusiness.net/tale-two-cities-brussels-and-washington-struggle-cooperate-science.
[674] See *Artificial Intelligence*, European Commission (last accessed Sept. 16, 2020), https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

data, infrastructure, networks, and communications across Europe, create a single European data space, and foster European technology innovation on a large scale.[675]

The United States and the EU should work together to overcome challenges, particularly to the full realization of joint R&D,[676] as strengthened cooperation on AI and emerging technologies strengthens democracy and other shared values, furthers the development of responsible AI that enhances human welfare, encourages innovation and economic growth, and advances global security.[677] Decreased cooperation between the United States and the EU only benefits strategic competitors and adversaries that seek to undermine free and open societies.

Potential opportunities for U.S.-EU collaboration span all areas of AI development and implementation and require a regular, high-level dialogue on AI and other emerging technologies.[678] The Commission proposes a Cabinet and Secretary-level Strategic Dialogue for Emerging Technologies (SDET), which should be separate from the annual Information Society Dialogue, and supplemented with working level meetings.[679] The SDET should be Led on the U.S. side by the Department of State, with participation of senior officials from the Departments of Defense, Energy, and Commerce, as well as the National Science Foundation. On the EU side, the SDET should be led by the European Commission with participation from the Directorate-Generals for Communications Networks, Content and Technology (DG CONNECT) and Research and Innovation (DG RTD), as well as EU member states, particularly from their foreign, defense, and relevant science or research ministries. Given the defense and security implications, relevant NATO interlocutors should also participate. Each meeting of the SDET should include an agenda for concrete action to align the United States and EU and implement mechanisms to expand collaboration.

The Commission will propose a SDET agenda in the final report that will address, among other items, potential joint R&D projects, including privacy-enhancing AI applications; the U.S. role in the EU's Horizon Europe and Digital Europe framework; data sharing to

[675] "Europe's ability to define its own rules and values in the digital age will be reinforced by such capacities. European technological sovereignty is not defined against anyone else, but by focusing on the needs of Europeans and of the European social model. The EU will remain open to anyone willing to play by European rules and meet European standards, regardless of where they are based." See *Shaping Europe's Digital Future,* European Commission at 3 (Feb. 2020), https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf; Frances G. Burwell & Kenneth Propp, *The European Union and the Search for Digital Sovereignty: Building a "Fortress Europe" or Preparing for a New World?*, Atlantic Council (June 2020), https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf; *High-Level Expert Group on Artificial Intelligence*, European Commission (last accessed Sept. 16, 2020), https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence; *A European Strategy for Data,* European Commission (Feb. 19, 2020), https://ec.europa.eu/info/files/communication-european-strategy-data_en.

[676] See Richard L. Hudson, *Tale of Two Cities: Brussels and Washington Struggle to Cooperate in Science*, Science Business (May 14, 2018), https://sciencebusiness.net/tale-two-cities-brussels-and-washington-struggle-cooperate-science.

[677] Christie Lawrence & Sean Cordey, *The Case of Increased Transatlantic Cooperation on Artificial Intelligence*, Harvard Kennedy School Belfer Center at 3 (Aug. 2020), https://www.belfercenter.org/publication/case-increased-transatlantic-cooperation-artificial-intelligence .

[678] The Commission notes that the EU and China held their first High-level Digital Dialogue on September 14, 2020. See *EU-China: Commission and China Hold First High-level Digital Dialogue*, European Commission (Sep. 10, 2020), https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1600.

[679] The Commission is aware that the United States and the European Union meet annually to discuss similar topics at the Information Society Dialogue (ISD). The Commission's recommended dialogue would include more senior level participants. See *Joint Statement on the 17th European Union - United States Information Society Dialogue,* European Commission (July 30, 2020), https://ec.europa.eu/digital-single-market/en/blogposts/joint-statement-17th-european-union-united-states-information-society-dialogue.

facilitate cross-border R&D, collaborative projects, and privacy-protecting data transfers; coordination of regulatory frameworks to promote U.S. and EU innovation, including alignment of export controls and investment screening; coordinated investments in emerging technologies; facilitation of talent exchanges; countering and competing against disinformation enabled by AI; countering intellectual property theft; and countering forced technology transfers.

Proposed Executive Branch Action

The Department of State, in partnership with the European Commission, should convene SDET, a regular, high-level (Commissioner and Secretary-level) dialogue on AI and other emerging technologies with supporting working level meetings. U.S. representation should include the Departments of Defense, Energy, and Commerce, as well as the National Science Foundation. EU member states and their respective foreign, defense, and science or research ministries, the European Commission's DG CONNECT and DG RTD, and relevant NATO interlocutors should also participate. The Department of State and European Commission should include an agenda for concrete action to align the United States and EU and implement mechanisms to expand collaboration.

Issue 2: Blueprint for AI Cooperation

Recommendation 11: The United States Government, led by the Department of State, should engage in high-level and working group meetings with select key partners and allies on concrete, operational AI projects and applications and use the proposed Blueprint for AI Cooperation to assess and identify areas to deepen the relationship.

For a sustained global AI cooperation effort to be effective, cooperation must lead to concrete, operational projects for the development and application of AI. As such, the Commission recommends to the Executive Branch and Congress a *Blueprint for AI Cooperation*, outlined in full in Annex B. The *Blueprint*, as summarized in Figure 2 below, contains proposals for cooperative endeavors and the ways to achieve them across eight critical areas.

Figure 5.2: Overview of Blueprint for Global AI Cooperation

CRITICAL AREA	OVERVIEW
1. DEFENSE & SECURITY COOPERATION (*See* Pillar I)	• Expand coalitions and existing alliances to incorporate AI into range of operations (logistics, humanitarian missions, intelligence, use of armed force, etc.) • Promote accelerated and responsible adoption of AI and dedicate personnel and resources to develop interoperable technology and expertise required to undertake operations reliant on advanced technology to enhance U.S. and international security • Address challenges unique to development and use of AI and emerging technologies for military purposes, with a focus on military interoperability
2. STANDARDS & NORMS DEVELOPMENT (*See* Pillar II)	• Engage proactively with coalition efforts to organize like-minded democratic nations around key AI-related issues – across all critical areas • Shape technical AI standards with focus on standards for privacy-enhancing technology, data sharing and labeling, interoperability, safety and reliability, and traceability • Promote U.S. national security through international standards development organizations
3. JOINT R&D	• Promote collaborative, cross-border R&D work among nations, industry, civil society, and academia • Pursue collaborative, cross-border R&D projects and application development with nations, industry partners, and researchers • Facilitate funding of joint R&D efforts where feasible • Develop comparative advantages, reduce redundancies, share best practices, and improve resource allocation • Focus on areas of shared interest (e.g., privacy enhancing technologies, next-generation materials, prototyping)
4. DATA-SHARING ECOSYSTEM	• Address legal and regulatory barriers to international collaborative work • Explore bilateral and multilateral, general and specific approaches to enable data sharing consistent with privacy and other fundamental values
5. INNOVATION ENVIRONMENT	• Collaborative efforts to align and develop regulatory and legal regimes in areas critical to fostering domestic and international innovation: o export controls, o investment screening, o supply chain assurance, o emerging technology investment, o trade policy, and o intellectual property
6. HUMAN CAPITAL	• Cooperative efforts to enable government, military, and private-sector talent exchanges • Domestic efforts to address immigration challenges to work and education opportunities
7. COUNTERING INFORMATION OPERATIONS	• Developing best practices and technology to address common threat of disinformation and other information operations • Pursue joint efforts to share information, develop technology, and coordinate efforts beyond intelligence agencies
8. AI TO BENEFIT HUMANITY	• Explore joint efforts to develop and deploy AI applications to benefit humanity at large through: o civilian space coordination; o AI-based foreign and democratic assistance; o smart cities and surveillance technology, o environmental science and energy, o cross-border health issues (inc. pandemic response), and o disaster response

The Commission is in the process of analyzing ways to increase AI cooperation with treaty allies and key partners and will submit its recommendations in the final report. These recommendations will build on promising recent developments designed to strengthen bilateral AI cooperation, such as the Declaration on Cooperation in Artificial Intelligence Research and Development with the UK.[680]

Proposed Executive Branch Action

The Commission recommends that the Department of State, in coordination with other relevant federal agencies, convene periodic, high-level dialogues with key allies and partners to pursue concrete, operational AI projects and applications on a bilateral or multilateral basis. The high-level dialogues should be supplemented by working group meetings designed to implement these projects and applications. The Commission will provide its specific recommendations for these bilateral dialogues in the final report.

[680] The Declaration, released following the September 25 inaugural meeting of the U.S.-UK Special Relationship Economic Working Group, formalizes the intention to establish a bilateral government-to-government dialogue to discuss "areas identified in this vision and explore an AI R&D ecosystem that promotes the mutual wellbeing, prosperity, and security of present and future generations." See *Declaration of the United States of America and the United Kingdom of Great Britain and Northern Ireland on Cooperation in Artificial Intelligence Research and Development: A Shared Vision for Driving Technological Breakthroughs in Artificial Intelligence*, U.S. Department of State (Sept. 25, 2020), https://www.state.gov/declaration-of-the-united-states-of-america-and-the-united-kingdom-of-great-britain-and-northern-ireland-on-cooperation-in-artificial-intelligence-research-and-development-a-shared-vision-for-driving/.

ANNEX A — Detail on Multilateral "Coalition of Coalitions" Strategy: Engage Multiple Efforts to Achieve Goals

EFFORT	CRITICAL AREAS	OBJECTIVES & CONSIDERATIONS	PRIORITY
D10	▪ Innovation Environment ▪ Emerging Technology	▪ Foster international cooperation to provide 5G alternatives to ZTE and Huawei, shift critical supply chains out of China, and protect national security ▪ Support nascent effort as it builds on the promising coalition (G7 plus Australia, India, and South Korea) and refines its goals, structure, and timeline; discuss potential for the UK and U.S. to jointly announce further developments ▪ Explore expansion of D10's focus into other emerging technologies critical to U.S. national security ▪ *Additional consideration: Divergent views on 5G and absence of key nations in 5G effort may limit efficacy on this issue*	I
FREEDOM ONLINE COALITION (FOC)	▪ AI to Benefit Humanity ▪ Standards & Norms Development	▪ Engage the 30+ country coalition (focused in Europe) as it seeks to publish a joint statement on AI and human rights, with a focus on content moderation and facial recognition, and builds up its Task Force on AI & Human Rights (T-FAIR) ▪ Continue to advance FOC's efforts on developing a call to action for countries "to promote rights-respecting AI technologies and reverse the trend of rising digital authoritarianism"	I
G20	▪ AI to Benefit Humanity ▪ Data-sharing Ecosystem ▪ Standards & Norms Development	▪ Advance efforts to enable international digital economy, develop global solution to tax challenges from digitization of the economy, and utilize tech in infrastructure and smart city efforts ▪ Ensure countries do not successfully promote authoritarian tech, particularly on topic of smart cities ▪ *Additional consideration: G20 includes China, Russia*	I
GPAI	▪ Standards & Norms Development ▪ Data-sharing Ecosystem ▪ Joint R&D ▪ Innovation Environment	▪ Influence direction, scope, goals of new multi-stakeholder effort ▪ Advance shared interests of democratic nations through working groups: 1) Responsible AI (including Ad Hoc AI and Pandemic Response Subgroup), 2) Data governance, 3) Future of Work, 4) Commercialization and Innovation ▪ Engage in Multi-stakeholder Experts Group Plenary ▪ Advocate for a U.S.-based center of expertise in addition to centers in Paris & Montreal to provide technical support for working groups ▪ Facilitate coordination of U.S. experts and representatives engaging in working groups and steering committee ▪ *Additional consideration: GPAI includes many but not all key partners*	I
ISO/IEC	▪ Technical Standards ▪ Data-sharing Ecosystem	▪ Advance standards to enable innovation, protect national and economic security ▪ Maintain consensus approach to standards development; counter adversarial or politicization efforts ▪ Ensure U.S. domestic policy and resourcing enables full U.S. engagement ▪ *Additional consideration: Domestic U.S. reforms could enhance U.S. position and ability to convey national security interests*	I
JAIC AI PART-NERSHIP FOR DEFENSE (AI PFD)	▪ Defense & Security ▪ Data-sharing Ecosystem ▪ Joint R&D ▪ Standards & Norms Development	▪ Continue to use AI PfD as a multilateral forum among the U.S. and 12 initial partner nations ▪ Continue "to promote the responsible use of AI, advance shared interests and best practices on AI ethics implementation, establish frameworks to facilitate cooperation, and coordinate strategic messaging on AI policy" ▪ Continue to expand and enhance AI PfD	I
NATO	▪ Defense & Security ▪ Data-sharing Ecosystem ▪ Human Capital	▪ Promote interoperability, human capital development, implementation of strategic objectives	I
OECD	▪ Standards & Norms Development ▪ Data-sharing Ecosystem ▪ Innovation Environment	▪ Continue articulating support of OECD's international efforts ▪ Continue to advance responsible AI, promote implementation of OECD Principles on AI, and develop a unified position on addressing practices that undermine principles ▪ Advance shared interests through AI Policy Observatory (OECD.AI) and the Network of Experts on AI (ONE AI), particularly in working groups on classifying AI systems, implementing values-based principles, and guiding national AI strategies ▪ Facilitate coordination of U.S. experts and representatives engaging in ONE AI and associated working groups ▪ Advance U.S. interests in "Going Digital" initiatives that promote data sharing and harmonizing on IP and regulation ▪ Facilitate coordination between OECD and GPAI ▪ *Additional consideration: OECD.AI, ONE AI members represent 30+ nations*	I
QUAD	▪ Defense and Security	▪ Build on the Quad framework to deepen AI cooperation and negotiate formal AI cooperation agreements in the Indo-Pacific	I
TTCP AISC	▪ Defense & Security ▪ Joint R&D	▪ Develop methods to address AI application and interoperability, including possible test bed for application in other situations and with other coalitions (e.g., NATO) ▪ *Additional consideration: The TTCP is limited to Five Eyes alliance members*	I

EFFORT	CRITICAL AREAS	OBJECTIVES & CONSIDERATIONS	PRIORITY
UN CCW GGE ON LAWS	▪ Defense & Security Cooperation ▪ Standards & Norms Development	▪ Advance shared interests of democratic nations regarding lethal autonomous weapons systems	I
WIPO & IP5	▪ Innovation Environment ▪ Intellectual Property ▪ Data-sharing Ecosystem	▪ Continue to engage in WIPO's "Conversations" on AI and IP Policy and Administration; includes data protection and sharing standards ▪ Continue to engage in IP5's New Emerging Technologies AI Task Force to advance global legal certainty and protections of AI-related IP, enhance efficiencies in office operations through AI adoption, and strengthen communication with industry	I
DEPT. OF STATE-LED INITIATIVES	▪ Innovation Environment ▪ Standards & Norms Development ▪ AI to Benefit Humanity	▪ Clarify goals and funding for State-led initiatives like the Clean Network programs ▪ Focus initiatives on creating a coalition of like-minded countries and companies built on trust principles and shared values that use "trusted" vendors and networks to protect citizens' privacy, secure sensitive data, and prevent IP theft ▪ Explore potential applications to supply chain assurance and providing alternative to BRI and Digital Silk Road ▪ Explore potential rebrand of effort to promote democratic tech, foster trust, and enhance coalition of democratic nations ▪ *Additional consideration: Initiatives may rise in priority as they are developed*	II
EAST ASIAN SUMMIT (EAS)	▪ Innovation Environment ▪ Emerging Technology	▪ Pursue as avenue to foster cooperation and stay abreast of Indo-Pacific regional developments. ▪ *Additional consideration: Bilateral relationships with many Indo-Pacific partners will remain critical with China, Russia participation in EAS*	II
G7	▪ Standards & Norms Development ▪ Innovation Environment	▪ Additional consideration: In 2019, the French government promoted the development of AI technologies, countering disinformation and other dangerous online content, and confidence-building in technological and data-based infrastructure. ▪ Success of D10 as a coalition to address common AI-related issues may limit G7 efficacy in the area though it continues to serve as a key forum to address important geopolitical topics.	II
IEEE	▪ Technical Standards	▪ Continue to engage, particularly on standards within the P7000 series on ethically aligned design series (e.g., P7001 - Transparency of autonomous systems and P7003 - Algorithmic Bias) and Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)	II
INTER-PARLIAMENTARY ALLIANCE ON CHINA (IPAC)	▪ Innovation Environment	▪ Influence IPAC to become vehicle for promoting AI-related goals of democratic nations, including the spread of democratic tech alternatives, alignment on emerging technologies that pose threats to national security, alignment on fair trade practices for digital commerce, countering IP theft, alignment on export controls and investment screening ▪ *Additional consideration: IPAC is an alliance of legislators from 17 nations (U.S., Japan, Uganda, and European nations); could serve as vehicle for aligning legislative priorities*	II
ITU-T	▪ Technical Standards ▪ AI to Benefit Humanity	▪ Continue to engage on international technical standards ▪ Engage in AI for Global Good Summit which has strong involvement from India, China, and Japan.	II
NATIONAL TECH. INDUSTRIAL BASE (NTIB)	▪ Innovation Environment ▪ Defense & Security ▪ Joint R&D	▪ Leverage NTIB to strengthen the industrial capabilities of the U.S. and allies; address supply chain concerns ▪ *Additional consideration: NTIB could serve as vehicle to advance AI-related interests around defense and security issues; members are Australia, Canada, U.S., UK*	II
T3	▪ Innovation Environment	▪ Support nascent effort as it promotes open, interoperable, reliable, and secure 5G ▪ Develop strategy to establish proofs of concept and explore collaborative approaches to AI and emerging technology	II
WORLD TRADE ORG. (WTO)	▪ Data-sharing Ecosystem ▪ Innovation Environment ▪ Trade	▪ Continue to engage in e-commerce and trade efforts outflowing from the 2019 Joint Statement on Electronic Commerce and the "Osaka Track," which promotes international rule-making to promote e-commerce and addresses data concerns	II
AFRICAN UNION (AU)	▪ AI to Benefit Humanity ▪ Innovation Environment ▪ Data-sharing Ecosystem	▪ Increase cooperation to support AU's Digital Transformation Strategy ▪ Stay abreast of efforts to develop and apply AI systems in Africa for socio-economic and other purposes as well the AU's goal to create a Digital Single Market by 2030	III
ASIA-PACIFIC ECONOMIC COOP. (APEC)	▪ Innovation Environment ▪ Emerging Technology	▪ Pursue as avenue to foster cooperation and stay abreast of Indo-Pacific regional developments; AI and data related efforts in APEC are very nascent ▪ *Additional consideration: USG may need to focus on bilateral engagements to achieve AI goals with many Indo-Pacific partners; APEC presents opportunities for US business participation*	III

EFFORT	CRITICAL AREAS	OBJECTIVES & CONSIDERATIONS	PRIORITY
ASSOC. OF SE ASIAN NATIONS (ASEAN)	▪ Innovation Environment ▪ Emerging Technology	▪ Pursue as avenue to foster cooperation and stay abreast of Indo-Pacific regional developments. ▪ *Additional consideration: Bilateral relationships with many Indo-Pacific partners will remain critical to advance AI-related efforts*	**III**
COUNCIL OF EUROPE (COE)	▪ Standards & Norms Development	▪ Continue to engage in their efforts to develop an international legislative framework on AI similar to the Budapest Convention on Cybercrime and support the Ad Hoc Committee on Artificial Intelligence (CAHAI) ▪ *Additional consideration: The U.S. is a non-voting observer*	**III**
ORG. FOR AMERICAN STATES (OAS)	▪ Innovation Environment	▪ Stay abreast of early efforts to coordinate on AI strategy	**III**
ORG. FOR SECURITY AND COOP. IN EUROPE (OSCE)	▪ AI to Benefit Humanity	▪ Stay abreast of efforts examining AI and its effects on freedom of expression and free speech	**III**
UN EDUC., SCI., AND CULTURAL ORG. (UNESCO)	▪ Standards & Norms Development	▪ Continue to engage on its development of a global standard-setting instrument on AI ethics	**III**
UNSG HIGH-LEVEL PANEL ON DIGITAL COOP.	▪ AI to Benefit Humanity	▪ Engage as part of UN engagement; however, it is unlikely the High-level Panel on Digital Cooperation (HLPDC) will be a main vehicle for advancing U.S. AI interests	**III**

ANNEX B — Blueprint for AI Cooperation

This Blueprint for Artificial Intelligence Cooperation sets out concrete, operational steps for a global artificial intelligence (AI) cooperative framework focused on bilateral and multilateral arrangements. It contains preliminary recommendations on potential AI projects or applications that would provide fertile ground for multilateral or bilateral cooperation along with considerations for implementing these projects or applications.

As the Commission continues its work towards its March 2021 final report, it intends to develop these concepts and apply them to key allies and partners of the United States.

Critical Area 1: Defense & Security Cooperation

Priorities for Cooperation within Existing Alliances

1. **Improving military interoperability across alliances.** Recognizing the differential adoption of advanced technology among members of alliances such as the North Atlantic Treaty Organization (NATO), pursue efforts to avoid a de facto decoupling between the United States and its allies which could hinder political cohesion and military effectiveness of the alliance and coalition operations.

    a. Efforts should include wargaming and experimentation to develop use cases and agreement on specific underlying data sets; exploration of machine learning-related approaches to stress test capabilities and operational concepts; development of common Test & Evaluation, Validation & Verification (TEVV) procedures; development of procedures for lifecycle data management—labelling, storage, accessibility, and security; and exploration of possibilities of privacy preserving machine learning (PPML) to overcome data protection, security, and privacy issues among allies and with partners.

    b. Alliances should explore pilot projects in low-risk areas, such as for enterprise AI applications (logistics and sustainment) to derive lessons that would support broader application of AI systems for alliance efforts.

2. **Development of data sharing policies and practices for collection, storage, use, and sharing of data across alliances.** In the NATO context, common data archival procedures could be pursued through NATO standardization agreements. Furthermore, NATO-EU cooperation will be required to ensure compatibility and alignment.

3. **Development of privacy-enhancing technologies.** Alliances require coordinated R&D on privacy-enhancing technologies as well as procedures to enable data sharing consistent with legal requirements in allies' legal jurisdictions.

4. **Alignment on standards and norms.** Alliances will require alignment and adoption of norms and standards to enable responsible, accelerated development of and access to AI applications for defense and security purposes as well as articulation

of and development for doctrine concerning responsible uses of AI-related technologies and autonomous systems.

5. **Development of human capital.** Alliances need to incorporate technical expertise to develop ways to more effectively inform decision-making about policies, doctrine, capabilities and resourcing that is better attuned to AI-related technologies, their benefits, costs and risks of development and adoption. Alliances should identify methods to improve expertise and access to sources of expertise and bridge the gap between the United States and its allies. Methods to define and track AI talent will be critical to determining needs and adopting methods to address those needs. Joint talent exchange programs should be explored to enhance allied talent base, including potential joint initiatives involving the NATO Defense College.

Additional Cooperation Priorities

1. **Development of formal AI cooperation agreements.** The United States Government should explore and pursue negotiation of formal AI cooperation agreements with partners and allies outside of NATO.

2. **Coordination on Lethal Autonomous Weapons Systems (LAWS).** The United States Government should coordinate with allies and partners to ensure that the development of norms, standards, and regulations on LAWS are consistent with shared values, U.S. military requirements, the law of armed conflict, and the rule of law.

Critical Area 2: Standards & Norms Development

International Technical Standards

In addition to the strategies for developing coalition efforts of the United States around AI and associated technologies, as addressed in Pillar II of this report, the United States Government should seek to align with allies and partners and prioritize efforts in development of international technical standards in the following areas:

1. Safety and reliability;

2. Privacy-enhancing technologies, including PPML, allied cryptographic code, and other privacy-enhancing technologies;

3. Data sharing, labelling, and related documentation for data, models, and systems;

4. Assessing system performance per shared values (including fairness, interpretability, reliability, and robustness);

5. Traceability, focused on audit trail requirements per mission needs for high-stakes AI systems including safety-critical applications; and

6. Interoperability including benchmarks that assess reliability of produced model explanations.

The United States Government's position on these should be guided by the Commission's *Key Considerations for Responsible Development and Fielding of AI* with a focus on U.S. national security and defense interests.

Critical Area 3: Joint Research & Development (R&D)

Cooperative Projects and Applications for International or Cross-Border R&D

1. **Development of privacy-preserving technology**, such as homomorphic encryption and differential privacy techniques,[681] to facilitate cross-border AI applications, data sharing, and cooperative efforts.[682]

2. **Development of TEVV systems** to strengthen the development of trustworthy, robust AI is critical to advancing interests of democratic nations to understand iterating AI systems in multi-agent/adversarial contexts.[683]

3. **Development of AI for modeling, simulation, and design** to provide researchers with a larger scope of AI-ready data sets.[684]

4. **Development of one- and few-shot learning algorithms**—algorithms that rely on less data—to facilitate future joint R&D and data sharing and improve context-specific interoperability.[685]

5. **Development of robust allied AI** to reduce vulnerabilities of allied AI systems and training data to adversarial attacks.[686]

6. **Achieving context-specific interoperability of AI systems** necessary for cross-border AI applications.[687] The potential for AI to increase speed of operations will require partners and allies to stress test decision making procedures and communications protocols to ensure interoperability. Interoperability of AI systems

[681] Collaborative research in this area could draw from promising R&D use cases, including the DARPA Brandeis program and the IARPA HECTOR program. See *Brandeis*, DARPA (last accessed Sept. 18, 2020), https://www.darpa.mil/program/brandeis; *Homomorphic Encryption Computing Techniques with Overhead Reduction (HECTOR)*, IARPA (last accessed Sept. 18, 2020), https://www.iarpa.gov/index.php/research-programs/hector; see also *Key Considerations* at 13 (recommending R&D to advance privacy-preserving technology).

[682] See *First Quarter Recommendations,* NSCAI at 11 (Mar. 2020), https://www.nscai.gov/reports.

[683] See *Key Considerations* at 29 (recommending R&D for TEVV of AI systems to improve TEVV and build checks and balances into an AI system). TEVV R&D includes complex system testing to improve understanding of and confidence in emergent performance of composed AI systems and improve methods to understand, predict, and control systems-of-systems to avoid negative outcomes resulting from system interaction. In addition, R&D in a multi-agent scenario will advance the understanding of interacting AI systems, including the application of game theory to varied and complex scenarios, and interactions between cohorts composed of a mixture of humans and AI technologies. See also *First Quarter Recommendations*, NSCAI at 11 (Mar. 2020), https://www.nscai.gov/reports.

[684] The Commission has previously recommended that the United States devote greater resources to AI modeling, simulation, and design. See *First Quarter Recommendations*, NSCAI at 6-13 (Mar. 2020), https://www.nscai.gov/reports.

[685] See *First Quarter Recommendations*, NSCAI at 11 (Mar. 2020), https://www.nscai.gov/reports.

[686] See *Key Considerations* at 22 (recommending R&D for AI security and robustness—to cultivate more robust methods that can overcome adverse conditions; advance approaches that enable assessment of types and levels of vulnerability and immunity; and to enable systems to withstand or to degrade gracefully when targeted by a deliberate attack); see also *First Quarter Recommendations*, NSCAI at 11 (Mar. 2020), https://www.nscai.gov/reports.

[687] See *Key Considerations* at 7, 29 (recommending collaboration among allies and partners to enable interoperability and trust).

is already an issue at the forefront of defense cooperation and will only grow in importance as technology matures.

7. **Development of AI to secure and improve resiliency of supply chains** to protect AI-component supply chains while promoting domestic and allied innovation and to apply AI to improve auditing, mapping, and securing supply chains while ensuring resilience to shocks. Given the inherently cross-border nature of supply chains and their critical role in the international economy around AI and advanced technology, this is a natural area for the United States to work collaboratively with like-minded nations.

Implementation Methods

Any of the projects identified above may be pursued not only on a government-to-government basis but also in partnership with industry, research centers, and other stakeholders. Coordinated R&D may, in most cases, be enabled through basic legal instruments or covered under an existing science and technology agreement between the United States and a foreign nation.

Yet the type of collaborative R&D projects the Commission contemplates presents opportunities to explore more lasting arrangements that could generate further collaboration and strengthen trust among partners. Accordingly, the United States Government, working with the private sector and research community, should explore the following concepts for facilitating a robust international collaborative infrastructure. Any of these would assist the United States Government and its allies and partners to pool resources, reduce redundancies, share best practices, and develop new capabilities.

1. **Development of an International Center of Excellence (ICE) drawing from multiple nations.** The ICE, with funding from all participating nations, could serve as a coordinating institution for joint R&D and data-sharing efforts involving AI and emerging technology—to include bilateral projects and those facilitated by GPAI and other multilateral and multi-stakeholder forums. This could be modeled on the EU Centres of Excellence, Canada's International Center of Expertise in Montréal for the Advancement of Artificial Intelligence (ICEMAI), and France's National Institute for Research in Digital Science and Technology (INRIA).[688]

[688] The European Union intends to establish Centres of Excellence and Digital Innovation Hubs focused on AI. ICEMAI works with the Government of Canada's Advisory Council on Artificial Intelligence, Forum IA Quebec, and the International Observatory on the Societal Impacts of Artificial Intelligence and Digital Technologies and is supported by the governments of Canada and Quebec with over $15 million in funding over five years. INRIA was launched in February 2020 and has a contract with the Government of France to focus on "speeding up development of France's scientific and technological leadership, as part of a Europe-wide approach," including prioritizing AI and other digital technologies to meet societal challenges, constructing European research and innovation spaces, strengthening the tech industrial base,, reinforcing public policies, and developing leading research universities. See *Communication Artificial Intelligence for Europe,* European Commission (May 25, 2018), https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe; *The Global Partnership on Artificial Intelligence Officially Launched*, Montreal International (June 15, 2020), https://www.montrealinternational.com/en/news/the-global-partnership-on-artificial-intelligence-officially-launched/; *INRIA: For Scientific, Technological and Industrial Leadership in Digital Technology*, Government of France (Feb. 24, 2020), https://www.gouvernement.fr/en/inria-for-scientific-technological-and-industrial-leadership-in-digital-technology.

2. **Creation of a joint emerging tech investment consortium.** Modeled on In-Q-Tel, the consortium would spur investment by the United States and foreign partners in early-stage companies to further development of AI technology that advances and/or protects democratic values. The effort would benefit the United States and its allies and partners through a cross-border platform to engage with start-ups and entrepreneurs in the AI and emerging tech space.

3. **Funding of an allied initiative to develop a certified cryptography code.** Penetration testing is an essential component of verifying the security, reliability, and novelty of PPML and AI software, yet it is costly. An allied initiative on certified cryptography would decrease costs by enabling penetration testers to test against the allied cryptographic code.

4. **Establishment of multilateral innovation prize competitions.** Modeled on Defense Advanced Research Projects Agency (DARPA) Challenges and XPRIZE Foundation competitions, international innovation prize competitions sponsored by two or more governments would incentivize R&D in fundamental AI or around specific applications necessary for national security and help to pool resources and talent with allies and industry.[689]

5. **Pursuit of allied research at U.S. national labs.** The United States should explore mechanisms for allied researchers to conduct research at U.S. national labs on sensitive topics. Although there are limitations on U.S. national labs to allow foreign researchers, domestically housed research efforts would limit concerns around cross-border data-sharing and cybersecurity and could prove fruitful in R&D necessary for defense and security applications.

6. **Development of an allied R&D matching platform.** The platform would connect researchers and their projects with funders and partners (governments, philanthropists, venture capitalists, companies, research institutions), providing the United States Government with increased visibility into research trends.

7. **Development of an international test bed for TEVV.** An international test bed for TEVV could be modeled on the National AI Research Institutes, but with a cross-border focus, and on the AI4EU project.[690]

8. **Collaboration between centers of excellence, research institutes, and industry consortia through additional coordination by partner governments.** This concept would leverage existing and soon to be established centers like European Union Centres of Excellence, European AI-related Digital Innovation Hubs, the U.S. National AI Research Institutes program, General

[689] *AI To Solve Global Issues*, XPRIZE (last accessed Sept. 18, 2020), https://www.xprize.org/prizes/artificial-intelligence.

[690] The National AI Research Institutes is a joint government effort among the National Science Foundation (NSF), U.S. Department of Agriculture (USDA) National Institute of Food and Agriculture (NIFA), U.S. Department of Homeland Security (DHS) Science & Technology Directorate (S&T), and the U.S. Department of Transportation (DOT) Federal Highway Administration (FHWA). See *National Artificial Intelligence (AI) Research Institutes*, NSF (last accessed Sept. 18, 2020), https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505686. The AI4EU project was founded by the European Commission under the H2020 program to establish the first European AI On-Demand Platform and Ecosystem. The Platform is designed to support the AU ecosystem and provide a forum to share AI resources from European projects. See *About the Project,* AI4EU (last accessed Sept. 18, 2020), https://www.ai4eu.eu/about-project.

Services Administration's AI Center of Excellence (in partnership with the Departments of Agriculture and Health and Human Services as well as the Joint Artificial Intelligence Center (JAIC)), the Alan Turing Institute in the United Kingdom, and the Montreal Institute for Learning Algorithms (MILA),[691] the Alberta Machine Intelligence Institute (AMII),[692] and the Vector Institute for Artificial Intelligence in Canada.[693] On the U.S. side, this could involve building on industry and academic efforts like the Stanford Institute for Human-Centered Artificial Intelligence.[694]

9. **Creation of a U.S. Center of AI Excellence.** Alternatively, the United States Government should explore creating its own Center of AI Excellence to enable collaboration among domestic and foreign centers of excellence, research institutes, and industry consortia.[695]

U.S. Domestic Considerations

Domestically, the United States should assess the appropriate roles for federal agencies with relevant responsibilities and coordinate efforts across the interagency to avoid duplication and deploy resources effectively and efficiently. Relevant agencies for the types of joint R&D projects contemplated in this blueprint include DARPA, Intelligence Advanced Research Projects Activity (IARPA), the National Science Foundation (NSF), and the Departments of State, Defense (DoD), Energy (DoE), and Commerce. The appropriate federal actor will depend on the nature of the project. In some cases, NSF's National AI Research Institutes may be most appropriate. Furthermore, federal agencies will need to coordinate with appropriate industry and academic partners within the United States and should explore not only inter-governmental collaboration but also collaboration with foreign research institutes, such as the Turing Institute (UK) and the Vector Institute (Canada).

Critical Area 4: Data Sharing Ecosystem

The frameworks that govern the sharing of data between the United States and different countries present barriers to collaborative R&D and to AI applications designed to achieve mutual interests. The United States must engage internationally with democratic nations that support strong privacy rights to examine the data sharing ecosystem and address legal and regulatory obstacles to collaboration. Coordinated approaches are critical to avoid ceding ground on AI and emerging technology to nations that do not adhere to the same

[691] *AI for Humanity,* Mila (last accessed Sept, 18, 2020), https://mila.quebec/ia-dans-la-societe/.

[692] *Artificial Intelligence For Good and For All*, Amii (last accessed Sept. 18, 2020), https://www.amii.ca/.

[693] See *CIFAR Pan-Canadian Artificial Intelligence Strategy*, CIFAR (last accessed Sept. 18, 2020), https://www.cifar.ca/ai/pan-canadian-artificial-intelligence-strategy; *About Us*, Vector Institute for Artificial Intelligence (last accessed Sept. 18, 2020), https://vectorinstitute.ai/about/.

[694] See Stanford Institute for Human-Centered Artificial Intelligence (last accessed Sept. 18, 2020), https://hai.stanford.edu/welcome.

[695] To attract involvement by foreign government and non-government organizations, the United States could consider incentives such as exemption from ITAR rules, fast-tracked visas, opportunities for researchers to continue to work in government or patent research if they will go to market with technology/application. Furthermore, to enable the Center of AI Excellence to generate truly collaborative innovation, implementation should consider methods to ensure that research remains open and easily leveraged by government and non-government members until such time as a research intends to go to market with an idea.

fundamental legal and ethical guideposts. There are various mechanisms to enable data sharing and these should be explored as part of efforts to coordinate on AI.

Implementing Data Sharing Arrangements

To facilitate data sharing, the Commission proposes that the United States Government, particularly the Departments of State and Commerce as well as Congress, explore the following mechanisms.

1. **A multilateral data free flow with trust (DFFT) agreement.** The United States Government should lead an effort to create a formal, potentially treaty-based approach to data sharing modeled on the DFFT concept introduced by Japan at the June 2019 G20 Summit. DFFT would permit the free flow of data between authorized parties upon meeting specific standards—including intellectual property (IP), privacy, and cybersecurity protections.[696] A *general* DFFT would require significant consideration of data protection, IP protection, privacy shield, and trade issues, both for the United States domestically and for foreign partners. A *specific* DFFT, on the other hand, focused on the free flow of data for particular purposes—such as facilitating pandemic response efforts—would have a greater chance of success and could be a model for targeted data sharing arrangements in other areas of shared interest.

2. **Ad hoc data sharing arrangements on bilateral or multilateral bases.** The United States should also explore the willingness of strategic allies and partners to engage in targeted, non-treaty data sharing arrangements. "Innovation sandbox" arrangements may be designed to facilitate specific challenges across all domains—security, health, disinformation, environmental resilience, and so on.

3. **Agreements to share specific data sets with specified foreign partners.** Narrower in scope to the above two approaches, an agreement of this kind would allow researchers from different countries to access the same data sets for their respective projects. For example, in the context of COVID-19 and health care,[697] countries would need to address data labelling, data storage, data anonymization, data security and other issues on a joint basis or through a pilot project. This type of effort could also include joint projects with allies to anonymize high-impact datasets for specific research or initiatives (such as National Institutes of Health datasets and datasets maintained, for various purposes, by DOE, the U.S. Agency for International Development (USAID), the Food and Drug Administration, DARPA, IARPA, and the Department of State's Center for Analytics).

4. **Agreement on foundational data documentation, labelling, and data organization frameworks at international organizations.** Data agreements among members of alliances (such as NATO) or other international organizations would facilitate support to collaborative R&D endeavors, for example, ongoing

[696] Remarks by Angel Gurria, OECD Secretary General, delivered at the 2019 G20 Leaders' Summer - Digital (AI, data governance, digital trade, taxation) (June 28, 2019), https://www.oecd.org/g20/summits/osaka/2019-g20-leaders-summit-digital-osaka-june-2019.htm.

[697] See *OpenMined's Efforts for the Coronavirus Pandemic: COVID Alert App, Private Set Interaction, A Differential Privacy Wrapper and Private Identity*, OpenMined (Apr. 1, 2020), https://blog.openmined.org/openmineds-efforts-for-the-coronavirus-pandemic/.

efforts at the Organisation of Economic Co-operation and Development (OECD) AI Policy Observatory and Global Partnership on Artificial Intelligence (GPAI).

5. **Development of shared data environments.** Development of pooled data storage centers, computational environments, and cloud and edge computing facilities to pool data from different sources for free use by credentialed researchers. An approach like this would prove particularly beneficial to improve data sharing among members to the Five Eyes alliance.

Numerous additional efforts can be identified to facilitate data sharing in different contexts. Notably, the solutions will depend on the particular uses and the stakeholders involved. Facilitating data sharing in a military-military context, for example, raises a different set of issues than data sharing in an industry-industry context.

Critical Area 5: Innovation Environment

The innovation environment refers to a set of issues dependent on regulatory and legal regimes, including: 1) export controls; 2) investment screening; 3) supply chain assurance; 4) emerging technology investment; 5) trade policy; and 6) intellectual property. This critical area addresses collaborative and/or coordinated work to align regulatory regimes and use regulatory levers to spur innovation—and protect associated development and deployment—in AI and other emerging technologies for commercial, government, and military uses. Aligning legal and regulatory regimes will also promote innovation in those nations.

Cooperation with key allies and partners will be instrumental in achieving AI-related goals across the suite of topics that are part of the innovation environment. In facilitating AI innovation, the GPAI working groups on the future of work and innovation and commercialization could be bolstered through bilateral cooperation with GPAI member states.

Export Controls & Investment Screening

In the *Second Quarter Recommendations*, the Commission recommended that the United States engage with allies and partners on legal reforms to (a) implement a coordinated approach to AI-related export controls and (b) enhance investment screening procedures.[698] The Departments of State and Commerce, on export controls, and the Departments of State and the Treasury, on investment screening, have already begun such work. Cooperation in these areas is critical to ensure that like-minded nations have the authority to unilaterally institute export controls and block predatory investments that present risks to national and international security.

The Commission has specifically recommended targeted, multilateral export controls on key, high-end semiconductor manufacturing equipment (SME) components.[699] In particular, the United States Government should engage the Netherlands and Japan to coordinate export controls on extreme ultraviolet and ArF immersion lithography tools, as doing so would limit the ability of China and other competitors to develop the high-end microelectronics that are increasingly essential for AI. Furthermore, as the Commission recommended last quarter,

[698] See *Second Quarter Recommendations*, NSCAI at 67-70 (July 2020), https://www.nscai.gov/reports.
[699] See Id. at 63-67.

the United States Government should also consider coordinating with allies and partners on export controls in targeted areas, such as for AI-specialized chips.[700]

Supply Chain Assurance

U.S. leadership in a variety of emerging technologies with national security implications, to include AI, is dependent on components sourced from U.S. strategic competitors or regions with significant geopolitical risk. This puts U.S. and allied access to these components in jeopardy during a crisis, increases the risk of strategic competitors exploiting vulnerabilities, and limits the ability of the United States Government to purchase trusted, bespoke components. The semiconductor manufacturing industry is a prime example of this challenge. While the United States must determine which components critical to AI and other emerging technologies are currently sourced from outside the United States and must be reshored, it should also examine which supply chains should be moved from strategic competitors to allied countries, and which can be sourced from anywhere in the world.

U.S. allies and partners have shared interest in developing a strategic, integrated, and multinational approach to supply chain coordination for critical technology components to enhance U.S. and allied security while reducing collective dependence of the United States on strategic competitors.

In addition, the United States Government should explore, in cooperation with allies and partners, a strategic plan to fund key chokepoint technologies and next-generation materials, approaches, and prototyping capabilities at discovery, manufacturing, and applied scales.[701]

Emerging Technology Investments

Likewise, investments in emerging technologies require coordinated action. 5G presents a test case for the challenges of international and multilateral coordination. Already the United States and partners have begun cooperating on developing alternatives to Chinese 5G infrastructure, including through the D10 as well as bilaterally. The Commission offered recommendations regarding steps to promote domestic development of 5G technology in its First Quarter Report and urged the United States to continue to work closely with key allies and partners on both constructive 5G technical solutions, and to ensure that global 5G networks are safe and secure.[702]

Trade Policy

While not a focus of U.S. efforts to date, trade policy is a key lever for the United States and foreign governments to promote an innovation environment. The United States should consider use of trade policy to further innovation by domestic and foreign industry particularly to further development of strategic partnerships, strengthening of national security, and facilitation of collaborative joint R&D efforts.

[700] See Id. at 57-58.

[701] See Id. at 48; Andrew Imbrie et al., *Agile Alliances: How the United States and its Allies Can Deliver a Democratic Way of AI,* Center for Security and Emerging Technology at 16-17 (Feb. 2020), https://cset.georgetown.edu/research/agile-alliances/.

[702] *First Quarter Recommendations*, NSCAI at 11 (Mar. 2020), https://www.nscai.gov/reports.

Intellectual Property

Intellectual property rights and regimes are critical to innovation in AI and emerging technologies. The following are possible initiatives to use the IP lever to further international collaboration. These could be explored through the WIPO's Conversation on AI and Intellectual Property, IP5, and forums with broader mandates. Bilateral engagements will be key in aligning practices to ensure the global environment promotes AI innovation and competitiveness. The Commission intends to explore these issues further in the Commission's final report.

1. **Assistance in developing strong IP and alignment in IP regimes.** The United States should assist partner nations in improving their IP regimes to help facilitate innovation while deterring IP theft. This may have the added benefit of deepening partnerships with allies; although like any foreign cooperation, would be suitable only with respect to certain countries. A more focused approach, through IP5 and WIPO, may prove more impactful in scope and could help to harmonize efforts to shore up IP with respect to identifiable international challenges.

2. **Domestic IP modernization.** The U.S. IP regime needs to be modernized as well as simplified to spur innovation in AI and other emerging technologies. Modernization of the U.S. IP regime will have the added effect of assisting the United States in promoting innovation and international dialogue.

3. **Joint efforts to stop IP theft.** IP theft remains a global concern.[703] With a goal of protecting the economic viability of AI innovation and emerging technologies, the United States should pursue a working group effort to develop a stronger international regime to address the export of counterfeit goods, theft of IP technology and forced technology transfers of foreign innovation.

[703] Eric Rosenbaum, *1 in 5 Corporations Say China has Stolen Their IP within the Last Year: CNBC CFO Survey,* CNBC (Mar. 1, 2019), https://www.cnbc.com/2019/02/28/1-in-5-companies-say-china-stole-their-ip-within-the-last-year-cnbc.html; Elizabeth Schulze, *Counterfeit Goods from China are Crushing American Small Businesses – and They're Calling on Trump to Fight Back,* CNBC (Feb. 29, 2020), https://www.cnbc.com/2020/02/28/small-businesses-are-pushing-trump-to-fight-chinese-counterfeits.html; Ben Wodecki, *Over 80% of EU Imported Fakes Come from China, Says Study,* Intellectual Property Magazine (Jan. 10, 2020), https://www.intellectualpropertymagazine.com/world/europe/over-80-of-eu-imported-fakes-come-from-china-says-study-139002.htm; Frank Dillon, *EU May be Losing €60bn in Annual Sales through IP Theft in Goods and Services,* Irish Times (June 6, 2019), https://www.irishtimes.com/business/innovation/eu-may-be-losing-60bn-in-annual-sales-through-ip-theft-in-goods-and-services-1.3914540; Masood Farivar, *US Intensifies Crackdown on China Intellectual Property Theft,* VOA News (May 15, 2020), https://www.voanews.com/usa/us-intensifies-crackdown-china-intellectual-property-theft; Daniel Gallington & Abraham Wagner, *Taking on China's Intellectual Property Theft,* The Washington Times (Feb. 5, 2019), https://www.washingtontimes.com/news/2019/feb/5/taking-on-chinas-intellectual-property-theft/; Julie Wernau, *Forced Tech Transfers are on the Rise in China, European Firms Say,* Wall Street Journal (May 20, 2019), https://www.wsj.com/articles/forced-tech-transfers-are-on-the-rise-in-china-european-firms-say-11558344240; Shaomin Li & Ilan Alon, *China's Intellectual Property Rights Provocation: A Political Economy View,* Journal of International Business Policy (Sept. 3, 2019), https://link.springer.com/article/10.1057/s42214-019-00032-x.

Critical Area 6: Human Capital

Human capital refers to the importance of ensuring that the United States and its allies cooperate on efforts to enable government, military, and private-sector talent exchanges and improve AI literacy and computer science education.

The United States and allies recognize increasing AI-related human capital requires building up domestic talent, bolstering their workforce's AI-related and digital literacy skills, strengthening AI training, attracting talent through immigration, and retaining the requisite talent across the public sector, private sector, and academia. This critical area addresses mechanisms for talent exchanges to further partners' AI capabilities and to enable sharing of best practices and expertise.

1. **International talent exchanges.** The United States and partner nations should develop different types of international talent exchanges to increase AI alignment, cross-pollinate ideas, and build AI-related skills and capabilities. For example, military officer exchanges to improve AI deployment and interoperability, including among NATO, JAIC, DoD, and foreign defense ministries and militaries; government-to-government exchanges of AI experts to assist in building tech and ethical expertise; exchanges to benefit industry-led multilateral and multi-stakeholder efforts like SDOs, GPAI, OECD and influence path taken by partners. Further, talent exchanges and secondments in industry and academia (both international industry-industry or academia-academia talent exchanges as well as government-industry/academia) would strengthen AI expertise (technical and ethical) and coordination between the United States and its allies and partners.

2. **Integrated recruiting among governments, industry, and academia.**

3. **Coordinating AI training development programs and sharing of best practices for government training and broader AI education programs (including in secondary schools and universities).** For example, the United States could coordinate on the "Artificial Intelligence and Analytics" in the EU's Digital Education Plan.

4. **Reform of U.S. immigration and visa laws to enable foreign researchers to travel to the United States for exchanges and training opportunities.** Reform of U.S. immigration and visa laws are critical to ensuring U.S. national security and furthering the interests of democratic nations around emerging technologies.[704]

Critical Area 7: Countering Malign Information Operations

The United States and strategic partner nations have a common interest in countering malign information operations. Joint efforts include detecting, moderating, identifying, and classifying malign information, developing standards and best practices, and training experts. This critical area addresses the growing international challenge of disinformation, compounded by the use of AI and machine learning (ML) technologies to facilitate

[704] The Commission plans to address immigration reform in its Final Report.

automation, with attention to coordinated efforts outside of the intelligence space to counter disinformation and other information operations.

1. **Create an International Task Force on Disinformation.** An International Task Force on Disinformation (ITFD) could be undertaken as a joint project between the United States and multiple countries, as well as the EU and NATO, to further joint efforts to enable content moderation and detection of disinformation, develop standards for identifying and classifying misinformation and disinformation, and train allies. Industry (e.g., Google, Facebook) and the academic and civil society (e.g., OpenAI) sectors would be important partners in this effort. The ITFD could draw best practices from, and should work in coordination with, the Global Internet Forum to Combat Terrorism.[705]

    a. The ITFD could also explore generating best practices for non-tech solutions, such as media literacy, free press, civic engagement initiatives. Several think tanks have done work in these areas, notably Center for Strategic and International Studies' Defending Democratic Institutions project and German Marshall Fund's Alliance for Securing Democracy.

    b. In the United States, among others, the Department of State's Global Engagement Center's (GEC) Technology Engagement Team (TET) could be a leader in this effort. TET conducts a tech-scouting process that vets and tests applications to counter disinformation. The Federal Bureau of Investigation's Foreign Influence Task Force (FITF), as the lead U.S. federal agency responsible for investigating foreign influence operations, could also help support this effort. Other relevant actors include the European External Action Services' Strategic Communication Task Force, the EU "Team Europe" initiative, and the NATO/StratCom Center of Excellence.

2. **Create a non-IC International Open Source Enterprise.** Develop international effort for timely collection of open source information and analysis of worldwide S&T developments to support decision-makers in allocating of R&D investment and/or divestment, promoting international collaboration and partnerships, detecting unwanted tech transfer, channeling hiring, supporting S&T forecasting, refining assessments of foreign S&T collection and intent, and supporting long-term S&T strategic planning for federal, and, as appropriate, sub-federal authorities, as well.

    a. Creation of an international Open Source Enterprise would likely require domestic U.S. legislation. Legislation would authorize establishment of an independent entity similar to the NSF. This entity would not be housed within the intelligence community or limited by Title 50 authorities. It would receive discrete appropriations for S&T collection, analysis, and decision support, with authority to support private and civil society actors, potentially through different public-private partnerships.

The GEC recently established a TET to conduct a tech-scouting process that vets and tests applications to counter malign information, and has developed an online open-source

[705] *Global Internet Forum to Counter Terrorism: Evolving an Institution*, GIFCT (last accessed Sept. 18, 2020), https://www.gifct.org/about/.

platform, "Disinfo Cloud"[706], where registered stakeholders including foreign governments can contribute and use a range of technology tools and programs designed to identify online propaganda and malign information. Finally, the Department of State's Public Affairs and Public Diplomacy officers require deeper training to compete against malign information.

Critical Area 8: AI to Benefit Humanity

This focus area addresses AI applications to benefit humanity and strengthen U.S. national security broadly conceived. These are project-specific applications that include joint efforts to address the following: 1) civilian space coordination; 2) foreign assistance needs around AI to counter competitive challenges and strengthen a coalition of democratic nations; 3) smart cities and surveillance technology; 4) environmental science and energy-focused projects; 5) cross-border health challenges including pandemic response efforts; and 6) disaster relief. Pursuing these partnerships will strengthen diplomatic and strategic ties with partner nations and resist efforts by undemocratic states to tie foreign assistance to adoption of AI technology that may be designed or deployed contrary to norms and values espoused by the United States and democratic nations.

Civilian Space Cooperation

The United States and other space agencies employ AI to tackle a range of space missions—including for visualization of space objects and situational awareness, tracking space debris for satellite collision avoidance, roving the lunar surface, deep space exploration with autonomous systems, and detection of asteroids that could threaten Earth.[707]

For safe satellite navigation around space debris, the European Space Agency (ESA) and the UK Space Agency both have AI initiatives underway, which suggest potential opportunities for closer U.S. collaboration.[708] ESA has already established a partnership with Stanford.[709] India is also building its space program and has deployed an AI-powered Moon rover.[710] Russia and China both appear to be working on technological solutions to the space collision problem, which could present an area for mutually beneficial cooperation. AI-enabled robotic assistants are also being developed for the International Space Station.[711]

Foreign Assistance to Support Economic Development and Democratic Values

The United States should look at foreign assistance in the area of AI, to include providing and subsidizing technology, mobile and digital infrastructure, research support to nations,

[706] *Disinfo Cloud*, U.S. Department of State (last accessed Sept. 18, 2020), https://www.state.gov/disinfo-cloud-launch/.

[707] On asteroids, see *Deep Asteroid*, NASA (May 27, 2016), https://open.nasa.gov/innovation-space/deep-asteroid/.

[708] *AI Challenged to Stave off Collisions in Space*, European Space Agency (Oct. 9, 2019), https://www.esa.int/Enabling_Support/Space_Engineering_Technology/AI_challenged_to_stave_off_collisions_in_space; Angelica Mari, *UK Government Seeks Innovations to Tackle Space Debris,* Computer Weekly (May 28, 2020), https://www.computerweekly.com/news/252483762/UK-government-seeks-innovations-to-tackle-space-debris.

[709] Andrew Myers, *Stanford Develops an AI Navigation System for a Future Satellite 'Tow Truck'*, Stanford News (Feb. 1, 2019), https://news.stanford.edu/2019/02/01/stanford-spurs-ai-navigation-space-rendezvous-software/.

[710] Leslie D'Monte, *Chandrayaan-2 Pragyan Shows How AI is Helping Space Exploration,* Mint (Sept. 6, 2019), https://www.livemint.com/technology/tech-news/chandrayaan-2-pragyan-shows-how-ai-is-helping-space-exploration-1567764065716.html.

[711] Mike Wall, *New, Emotionally Intelligent Robot CIMON 2 Heads to Space Station*, Space.com (Dec. 5, 2019), https://www.space.com/cimon-2-artificial-intelligence-robot-space-station.html.

and advising partner countries on best practices for developing national AI plans and strategies. This could be done unilaterally or in concert with other democratic nations. Potential allied partners could include the Japanese Bank for International Cooperation that has begun funding telecommunication infrastructure projects.[712] There are existing initiatives in the United States Government including the U.S. Agency for International Development's (USAID) Digital Strategy program, the nascent Economic Prosperity Network launched by the Department of State, and the U.S. International Development Finance Corporation.[713] In addition, the Department of State should incorporate AI-based technology into its ongoing efforts to promote internet freedom and counter censorship across the world, particularly at the Freedom Online Coalition (FOC).[714] Further applications could be developed, for example, by engaging with the International Committee of the Red Cross to explore extension of JAIC capabilities to apply AI to humanitarian relief operations.

Development and Use of Smart Cities/Surveillance Tech

Smart cities and surveillance technologies are an important area for international efforts in support of a democratic alternative to Chinese efforts in this space.[715] Efforts around this technology could be structured in different, non-exclusive ways: as a government-led project; as an industry-led project; through an XPRIZE-like challenge; and/or through a collaboration among technical experts. Potential stakeholders for such a project include NSF, the National AI Research Institutes, DARPA, NIST, various EU Centres of Excellence, research institutions (such as the Johns Hopkins University Applied Physics Laboratory, the Massachusetts Institute of Technology Computer Science & AI Laboratory, and the Stanford Institute for Human-Centered AI), GPAI, and non-governmental organizations such as OpenMined.

Environmental Sciences/Energy Focused Joint Project

There are many opportunities to pursue joint environmental and energy-focused AI projects to further partnerships with allies and facilitate data-sharing and joint R&D, recognizing the growing view that environmental degradation and climate change represent imperatives for national and international security. Projects could address renewable energy as part of the EU's Green New Deal, as a government-led initiative or a collaboration within Horizon 2020/Horizon Europe/Digital Europe.

[712] See *Infrastructure*, Japan Bank for International Cooperation (last accessed Sept. 18, 2020), https://www.jbic.go.jp/en/business-areas/sectors/infrastructure.html.

[713] See *Digital Strategy 2020-2024*, U.S. Agency for International Development (last accessed Sept. 23, 2020), https://www.usaid.gov/sites/default/files/documents/15396/USAID_Digital_Strategy.pdf.

[714] The Department of State's Internet Freedom and Business & Human Rights Section (IFBHR), within the Bureau of Democracy, Human Rights, and Labor, leads United States Government policy and engagement to protect human rights online. See *Internet Freedom: Fact Sheet*, Department of State (last accessed Sept. 19, 2020), https://www.state.gov/internet-freedom. IFBHR works across the United States Government, with democratic nations, with civil society, and with the Freedom Online Coalition (see **Annex A**). IFBHR's program includes funding development of censorship-defeating peer-to-peer communications technologies. See *Internet Freedom: Advancing and Promoting Peer-to-Peer Communications Technologies,* Dept. of State (last accessed Sept. 19, 2020), https://www.state.gov/internet-freedom-advancing-and-promoting-peer-to-peer-communications-technologies/.

[715] Kara Frederick, *The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem*, CNAS (Sept. 3, 2020), https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem.

The Department of Energy has several projects that could serve as a model for an international project around environmental sciences, including:

- the Partnership between Cross Section Evaluation Working Group and OECD's Nuclear Energy Agency's (NEA) Working Party on International Nuclear Data Evaluation Co-operation on International Criticality Safety Benchmark Evaluation Project, which uses machine learning (ML);[716]

- GEOTHERMICA, a collaboration among 12 European countries and the United States to fund AI specific research on geothermal R&D;[717] and

- the International Partnership for Hydrogen & Fuel Cells in the Economy (IPHE),[718] an intergovernmental partnership to facilitate and accelerate transition to clean & efficient energy with the support of AI/ML research.

Health-related Joint Projects

There are many opportunities to develop global collaborations around health-related projects, as the COVID-19 crisis has made clear. In a separate section of this report the Commission has specifically examined the intersection of AI and biotechnology policy, and recommends pursuing global cooperation on smart disease monitoring.[719] Such a global initiative, for example, could seek to combine existing data on zoological spills with open source health-related data to create shared, predictive, global disease monitoring models.

In addition, individual members of this Commission, in connection with work on the COVID-19 crisis, have endorsed a series of recommendations to develop AI applications and use AI for pandemic preparedness, vaccine development, and syndromic surveillance.[720] Several of these are particularly suitable for international or cross-border collaboration:

[716] Shuichi Tsuda, *The Working Party on Nuclear Criticality Safety (WPNCS),* OECD Nuclear Energy Agency (July 22, 2020), https://www.oecd-nea.org/science/wpncs/; *International Co-operation in Nuclear Data Evaluation: An Extended Summary of the Collaborative International Evaluated Library Organisation (CIELO) Pilot Project, NEA No. 7489,* OECD Nuclear Energy Agency (2019), https://www.oecd-nea.org/science/wpec/documents/volume40.pdf.

[717] GEOTHERMICA combines financial resources and expertise on geothermal energy research and innovation from 16 countries and their regions. It "launches joint projects that demonstrate and validate novel concepts of geothermal energy deployment within the energy system, and that identify paths to commercial large-scale implementation." One of the three focus areas includes "smart integration into the energy system and operations." Some of the projects have big data and smart system aspects, such as the French National Project through the Geothermica HEATSTORE project. GEOTHERMICA partners, like the U.S. Lawrence Livermore National Laboratory, have expertise in machine learning. See *About Geothermica,* Geothermica (last accessed Sept. 18, 2020), http://www.geothermica.eu/about-geothermica/; *French National Project,* HEATSTORE through Geothermica (last accessed Sept. 18, 2020), https://www.heatstore.eu/national-project-france.html; *American Partners,* Geothermica (last accessed Sept. 18, 2020), http://www.geothermica.eu/matchmaking/united-states/.

[718] Members of the partnership include the United States as well as Australia, China, Germany, Japan, Russia, Austria, Costa Rica, Iceland, ROK, South Africa, Brazil, India, the Netherlands, Canada, France, Italy, and Norway. See International Partnership for Hydrogen and Fuel Cells in the Economy, U.S. Department of Energy (last accessed Sept. 18, 2020), https://www.energy.gov/eere/fuelcells/international-partnership-hydrogen-and-fuel-cells-economy; International Partnership for Hydrogen and Fuel Cells in the Economy, IPHE (last accessed Sept. 18, 2020), https://www.iphe.net/.

[719] See Tab 4 of this memo, Recommendation #1.4.

[720] Jason Matheny, et al., *The Role of AI Technology in Pandemic Response and Preparedness: Recommended Investments and Initiatives*, NSCAI (June 25, 2020), https://www.nscai.gov/reports.

1. Development and coordination on international norms and standards to govern use and sharing of international health data, protecting privacy while ensuring timely accessibility of data;

2. Development of privacy standards for genomic datasets;

3. Increased international cooperation in the COVID-19 High Performance Computing Consortium (potentially through GPAI); and

4. Facilitation of international cooperation with DARPA's work on creating the infrastructure and protocols for data sharing and collaboration at the point of experimentation for drug discovery.

The National Nanotechnology Initiative's U.S.-EU Communities of Research[721] is a helpful model for an international effort. Many of the partner nations discussed in this report have launched health-related AI efforts, and those national efforts could provide a basis for important applications that benefit the United States and the international community.[722]

Disaster Relief

Climate and weather-related disasters like hurricanes, wildfires, and flooding are on the rise and AI is already being applied to mitigate the effects by locating survivors using unmanned aerial vehicles; removing debris after a disaster, deploying robots to communicate with victims, employing edge technology to obtain the most up to date data, running predictive simulations and leveraging social media reporting. The DoD is partnering with DoE and Microsoft to develop "deep-learning artificial intelligence algorithms to provide near-real-time data to improve the decision-making of first responders engaged in natural disasters and humanitarian assistance efforts"[723] and countries like Singapore are working with the JAIC on this particular National Mission Initiative.[724] The World Economic Forum has noted 160 million people a year are at risk from natural disasters and sees great benefit in AI from "reducing the time to assess damage to monitoring social media to more quickly and effectively deliver aid" while "sharpen[ing] the decisions of relief workers on the front lines."[725] The Forum has called for greater international collaboration in order to realize the benefits of AI to specifically include the area of disaster relief.

---

[721] *NanoEHS CORs,* US-EU Nanotechnology Communities of Research (CORs) (last accessed Sept. 18, 2020), https://us-eu.org/communities-of-research/.
[722] See, e.g., Jeff Mason, et al., *An Overview of Clinical Applications of Artificial Intelligence*, Canadian Agency for Drugs and Technologies in Health (Sept. 2018), https://www.cadth.ca/sites/default/files/pdf/eh0070_overview_clinical_applications_of_AI.pdf.
[723] David Vergun, *DOD Partners With Agencies to Use AI for Disaster Relief, Humanitarian Relief*, DOD News (Aug. 20, 2020), https://www.defense.gov/Explore/News/Article/Article/2319945/dod-partners-with-agencies-to-use-ai-for-disaster-humanitarian-relief/.
[724] Prashanth Parameswaran, *What's in the New US-Singapore Artificial Intelligence Defense Partnership?*, The Diplomat (July 1, 2019), https://thediplomat.com/2019/07/whats-in-the-new-us-singapore-artificial-intelligence-defense-partnership/.
[725] Ashley van Heteren, et al., *Natural Disasters are Increasing in Frequency and Ferocity. Here's How AI Can Come to the Rescue*, World Economic Forum (Jan. 14, 2020), https://www.weforum.org/agenda/2020/01/natural-disasters-resilience-relief-artificial-intelligence-ai-mckinsey/.

ANNEX C — Alignment of NSCAI Key Considerations for the Responsible Development and Fielding of AI with AI Ethics Principles

The table below illustrates how Department of Defense artificial intelligence (AI) principles[726] that would enable shared trust among NATO members can be operationalized through NSCAI's *Key Considerations for Responsible Development and Fielding of AI*. It also illustrates practices that would further support interoperability among allies. In the table below, an "X" indicates that the NSCAI recommended practice on the left operationalizes the AI principle at the top.

NSCAI Recommended Practices:		DOD PRINCIPLES OF AI ETHICS					NATO ALIGNMENT PRIORITY
		Responsible	Equitable	Traceable	Reliable	Governable	Interoperable
Core Values	A1 - Employ technologies and operational policies for privacy, fairness, inclusion, human rights, and LOAC	X	X			X	
	B1 - Consider and document value considerations based on how tradeoffs with accuracy are handled	X	X	X	X		
	B2 - Consider and document value considerations in systems that rely on representations of objective or utility functions	X	X	X	X		
	B3 - Conduct documentation, reviews, and set limits on disallowed outcomes	X	X	X	X	X	
Engineering	1 - Concept of operations development, and design and requirements definition and analysis	X	X	X	X	X	
	2 - Documentation of the AI lifecycle			X			X
	3 - Infrastructure to support traceability, including auditability and forensics		X	X			
	4 - Security and robustness: addressing intentional and unintentional failures				X	X	
	5 - Conduct red-teaming				X		
System Performance	A1 - Standards for metrics & reporting	X	X	X	X		X
	A2 - Representativeness of data and model for the specific context at hand	X	X	X	X		
	A3 - Evaluating an AI system's performance relative to current benchmarks			X		X	
	A4 - Evaluating aggregate performance of human-machine teams	X					
	A5 - Reliability and robustness	X		X	X		
	A6 - For systems of systems, testing machine-machine/multi-agent interaction	X			X		X
	B1 - Specifying maintenance requirements	X	X	X	X		
	B2 - Continuously monitoring and evaluating AI system performance	X	X	X	X	X	
	B3 - Iterative and sustained testing and validation	X			X	X	
	B4 - Monitoring and mitigating emergent behavior	X			X	X	X
Human-AI Interaction	A1 - Define functions and responsibilities of human operators and assign them to specific individuals	X		X			
	A2 - Policies should define the tasks of humans across the AI lifecycle	X					
	A3 - Enable feedback and oversight to ensure that systems operate as they should	X			X		
	B1 - Human-AI design guidelines	X	X	X		X	
	B2 - Algorithms and functions in support of interpretability and explanation	X		X		X	
	B3 - Designs that provide cues to human operator(s) about the confidence a system has in its results or behaviors	X		X		X	
	B4 - Policies for machine-human handoff	X		X		X	
	B5 - Leveraging traceability to assist with system development and understanding	X		X	X	X	
	B6 - Training	X	X	X	X	X	
Accountability/ Governance	1 - Identify responsible actors	X		X		X	
	2 - Adopt technology to strengthen accountability processes and goals	X		X		X	
	3 - Adopt policies to strengthen accountability	X		X			
	4 - External oversight support			X			

[726] See C. Todd Lopez, *DoD Adopts 5 Principles of Artificial Intelligence Ethics*, Department of Defense (Feb. 5, 2020), https://www.defense.gov/Explore/News/Article/Article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/.

APPENDIX I — Legislative Language

The below legislative text represents the Commission staff's best efforts to capture the Commission's third quarter recommendations. The Commission defers to the House and Senate members, staff, and legislative counsels as to appropriate drafting and policy.

TAB 1 — Legislative Language

Recommendation 1: Create an AI Innovator Award Program to Invest in Top Talent

and

Recommendation 2: Invest in Research Teams Pursuing Transformative Ideas in AI

SEC. ___.—ARTIFICIAL INTELLIGENCE AWARD PROGRAM.—

(a) ARTIFICIAL INTELLIGENCE INNOVATOR AWARD.—

(1) IN GENERAL.—The Director of the National Science Foundation shall partner with a nonprofit organization as described in subsection (c) to establish an Artificial Intelligence Innovator Award program to recognize and support the research of leaders in the field of artificial intelligence.

(2) ARTIFICIAL INTELLIGENCE INNOVATOR AWARD RECIPIENTS.—The Artificial Intelligence Award Selection Committee as described in subsection (d) shall select no fewer than 10 and no more than 20 award recipients each year. Recipients shall be selected for five-year, renewable award terms, based on a proven track record of prior innovation, a proposed general research program, a commitment to spend 75 percent of the recipients' time on research, and the committee's assessment of the potential of the research to generate breakthroughs in the area of artificial intelligence. Award amounts shall be determined by the selection committee with the objective of covering the full salary and benefits of the researcher and the cost of associated support staff and research equipment.

(b) ARTIFICIAL INTELLIGENCE TEAM AWARD.—

(1) IN GENERAL.—The Director of the National Science Foundation shall partner with a nonprofit organization as described in subsection (c) to establish an Artificial Intelligence Team Award program to support interdisciplinary research directed at applying artificial intelligence to solve complex problems or pursuing

use-inspired basic research efforts to advance a fundamental understanding of the science of artificial intelligence in a manner that provides a significant benefit to society.

(2) ARTIFICIAL INTELLIGENCE TEAM AWARD RECIPIENTS.—The Artificial Intelligence Innovator Awards Selection Committee as described in paragraph (d) shall select no fewer than five and no more than 10 team recipients each year. Recipients shall be selected for five-year, nonrenewable terms, based on team qualifications, commitment to multi-disciplinary approaches, and innovative research proposals. Award amounts shall be determined by the selection committee with the objective of covering the cost of carrying out the proposed research proposal.

(c) NONPROFIT ORGANIZATION PARTNER.—The National Science Foundation shall partner with a nonprofit organization active in the field of computer science and artificial intelligence that maintains the requisite expertise and connections to the artificial intelligence research community to identify promising talent and invest in innovative ideas and to manage the award programs described in subsections (a) and (b), including to administer the programs and arrange the annual meeting.

(d) ARTIFICIAL INTELLIGENCE AWARD SELECTION COMMITTEE.—Recipients of the Artificial Intelligence Innovator Award and the Artificial Intelligence Team Award shall be selected by a rotating committee of artificial intelligence experts known as the Artificial Intelligence Award Selection Committee. The Committee shall consist of members chosen for their first-hand experience in artificial intelligence research and their familiarity with the frontiers of the field. Committee member selection shall be made by the nonprofit organization partner identified under subsection (c) in consultation with the Director of the National Science Foundation or designee.

(e) ANNUAL MEETING.—The Director of the National Science Foundation shall sponsor an annual meeting of recipients of the Artificial Intelligence Innovator Award and the Artificial Intelligence Team Award, at which the award recipients shall share information on the progress of their work.

(f) OTHER SOURCES OF FUNDING.—Nothing in this section shall be interpreted to preclude a recipient of an Artificial Intelligence Innovator Award or an Artificial Intelligence Team Award from pursuing supplemental government research grant or other research support provided by individuals, nonprofits and corporations, provided that such additional funding does not interfere with the recipient's commitment to the research program or require the assignment of ownership of intellectual property in a manner that would be inconsistent with the provisions of the Bayh-Dole Act, Public Law 96-517.

(g) INDEPENDENT REVIEW.—The Director of the National Science Foundation shall engage an independent entity to conduct a review to assess the successes and failures of the awards program authorized by this section, evaluate the impact of the funding level and award term on the research conducted by participants, and recommend any needed changes to the program (including any expansion or contraction in the number of awards). The findings of the independent review shall be delivered to Congress not later than seven years after the commencement of the program.

(h) AUTHORIZATION OF APPROPRIATION.—

(1) There is authorized to be appropriated for each of the fiscal years 2022 through 2028 $125 million for the Artificial Intelligence Innovator Award.

(2) There is authorized to be appropriated for the Artificial Intelligence Team Award—

(A) $50 million for fiscal year 2022;

(B) $100 million for fiscal year 2023;

(C) $150 million for fiscal year 2024;

(D) $200 million for fiscal year 2025; and

(E) $250 million for fiscal years 2026 through 2028.

TAB 2 — Legislative Language

Recommendation 2: USD(R&E) should be appointed the Co-Chair and Chief Science Advisor to the Joint Requirements Oversight Council (JROC) for Joint and cross-domain capabilities to better synchronize warfighters and technologists and apply AI-enabled technologies to solve urgent operational challenges.

SEC. ___.—ENHANCED ROLE OF UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING ON THE JOINT REQUIREMENTS OVERSIGHT COUNCIL.—Section 181 of title 10, United States Code is amended—

(1) in subsection (b), by.—

(A) inserting "the Secretary of Defense and" before "the Chairman of the Joint Chiefs of Staff";

(B) redesignating paragraphs (2) through (6) as paragraphs (3) through (7);

(C) inserting a new paragraph (2), as follows:

"(2) leveraging awareness of global technology trends, threats, and adversary capabilities to address gaps in joint military capabilities and validate technical feasibility of requirements developed by the military services;"; and

(D) in redesignated paragraphs (4)(B) and (5) by inserting "the Secretary of Defense and" before "the Chairman of the Joint Chiefs of Staff";

(2) in subsection (c), by—

(A) striking "Chairman of the Joint Chiefs of Staff for making recommendations about" in paragraph (1)(A) and inserting "Council for";

(B) redesignating subparagraphs (B) through (E) of paragraph (1) as subparagraphs (C) through (F);

(C) adding a new paragraph (1)(B), as follows:

"(B) The Under Secretary of Defense for Research and Engineering, who is the co-Chair of the Council and is the Chief Science Advisor to the Council."; and

(D) by amending paragraph (3) to read as follows:

"(3) In making any recommendation to the Secretary and the Chairman of the Joint Chiefs of Staff pursuant to this section, the Co-Chairs of the Council shall provide any dissenting view of members of the Council with respect to such recommendation."; and

(3) in subsection (d), by—

(A) striking subparagraph (1)(D); and

(B) redesignating subparagraphs (E) through (H) of paragraph (1) as paragraphs (D) through (G).

Recommendation 3: USD(R&E) should have a dedicated fund to mature, operationally prototype, and transition exceptionally promising AI-enabled technologies.

SEC. ___.—ARTIFICIAL INTELLIGENCE DEVELOPMENT AND PROTOTYPING FUND.—

(a) IN GENERAL.—The Secretary of Defense shall establish a fund to be known as the "Artificial Intelligence Development and Prototyping Fund" to support operational prototyping and speed the transition of artificial intelligence-enabled applications into both service-specific and joint mission capabilities. The Fund shall be managed by the Under Secretary of Defense for Research and Engineering, in consultation with the Joint Artificial Intelligence Center, the Joint Staff, and the military services.

(b) TRANSFER AUTHORITY.—Amounts available in the Fund may be transferred to a military department for the purpose of carrying out a development or prototyping program selected by the Under Secretary of Defense for Research and Engineering for the purposes described in paragraph (1). Any amount so transferred shall be credited to the account to which it is transferred. The transfer authority provided in this subsection is in addition to any other transfer authority available to the Department of Defense.

(c) CONGRESSIONAL NOTICE.—The Under Secretary of Defense for Research and Development shall notify the congressional defense committees of all transfers under paragraph (2). Each notification shall specify the amount transferred, the purpose of the transfer, and the total projected cost and estimated cost to complete the acquisition program to which the funds were transferred.

Recommendation 4: Within ODNI, the Director of S&T should be designated as the IC's CTO and empowered to enable the IC to adopt AI-enabled applications to solve operational intelligence requirements.

and

Recommendation 6: The IC CTO should establish common technical standards and policies necessary to rapidly scale AI-enabled applications across the IC.

SEC. ___.—CHIEF TECHNOLOGY OFFICER FOR THE INTELLIGENCE COMMUNITY.—Section 2020 of title 50, United States Code is amended—

(1) in subsection (a), by striking "who shall be appointed by the Director of National Intelligence" and inserting "who shall be appointed by the Director of National Intelligence and shall serve as the Chief Technology Officer for the Intelligence Community."; and

(2) in subsection (c), by—

(A) redesignating paragraphs (2) through (5) as paragraphs (4) through (7); and

(B) inserting new paragraphs (2) and (3), as follows:

"(2) establish policies for the intelligence community on research and engineering, technology development, technology transition, prototyping activities, experimentation, and developmental testing, and oversee the implementation of such policies;

"(3) establish common technical standards and policies necessary to rapidly scale artificial intelligence-enabled applications across the intelligence community;".

Suggested Conference Report Language to Accompany Recommendations 4 and 6: The Chief Technology Officer for the Intelligence Community shall collect information on each Intelligence Community element's compliance with applicable standards and policies for artificial intelligence research and development, and shall provide such information to the Director of National Intelligence. The Intelligence Committees encourage the Director of National Intelligence to closely review the compliance information and place a temporary hold on an

Intelligence Community element that fails to execute artificial intelligence research and development funds in accordance with the applicable standards and policies.

Recommendation 5: The IC CTO, in coordination with USD(R&E), should develop a technology annex to the National Intelligence Strategy that establishes technology roadmaps to adopt AI-enabled applications to solve operational intelligence requirements.

SEC. ___.—TECHNOLOGY ANNEX TO THE NATIONAL INTELLIGENCE STRATEGY.—Section 3042 of title 50, United States Code is amended—

(1) by striking "and" at the end of paragraph (b)(7);

(A) redesignating paragraph (b)(8) as paragraph (b)(9); and

(B) adding a new paragraph (b)(8), as follows:

"(8) include a technology annex, developed by the Chief Technology Officer for the Intelligence Community in consultation with the Under Secretary of Defense for Research and Engineering, which provides a roadmap to adopt artificial intelligence-abled applications to address operational intelligence requirements;".

Recommendation 7: The IC should develop a coordinated and federated approach to applying AI-enabled applications to open source intelligence.

SEC. ___.—COORDINATED AND FEDERATED APPROACH TO APPLYING ARTIFICIAL INTELLIGENCE-ENABLED APPLICATIONS TO OPEN SOURCE INTELLIGENCE.—

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit a report to the congressional committees on intelligence providing detail on a coordinated and federated approach to applying artificial intelligence-enabled applications to open source intelligence and integrating that into existing intelligence processes and products. The report shall reflect input from heads of the intelligence community and shall address the items set forth in subsection (b). The report may be submitted with a classified annex.

(b) CONTENTS REQUIRED.—The report and approach required by subsection (a) shall address—

(1) the development of common standards and policies that enable the individual agencies to be more effective, such as contracting publicly available data sources for common use across the intelligence community and clarifying or updating policy guidance on the appropriate use of publicly available and open

source information, including with respect to privacy and civil liberties for U.S. persons or entities;

(2) the expansion of science and technology intelligence collection and analysis on dual-use "emerging & disruptive technologies";

(3) the identification of reliable industry partners across the spectrum of information sources and creating contract vehicles to rapidly integrate them into intelligence work across the intelligence community (including a pilot project to test "data-for-tools" exchanges in public-private partnerships);

(4) the coordination of government and non-government entities to communicate emerging risks and threats to industry and academia;

(5) the development of a robust capability for bringing in individuals without security clearances or awaiting security clearance adjudication and allowing them to work on unclassified projects that directly support the intelligence community;

(6) an implementation plan for how the intelligence community will implement the approach; and

(7) recommendations for such legislative and administrative action, including conforming and other amendments to the law, as the Director considers appropriate and necessary to implement the plan.

TAB 3 — Legislative Language

Recommendation 1.6: Accelerate Existing Occupational Series Initiatives

SEC. ___.—NEW OCCUPATIONAL SERIES FOR DIGITAL CAREER FIELDS.—Not later than 270 days after the date of the enactment of this Act, the Director of the Office of Personnel Management shall exercise its authority under section 5105 of title 5, United States Code to establish one or more new occupational series and associated policies covering Federal Government positions in the fields of software development, software engineering, data science, and knowledge management.

Recommendation 1.7: Create an AI Occupational Series

SEC. ___.—NEW OCCUPATIONAL SERIES FOR ARTIFICIAL INTELLIGENCE.—Not later than 270 days after the date of the enactment of this Act, the Director of the Office of Personnel Management shall exercise its authority under section 5105 of title 5, United States Code to establish a new occupational series and associated policies covering Federal Government positions in the field of artificial intelligence.

Recommendation 1.10: Create Digital Talent Recruiting Offices

SEC. ___.—DIGITAL TALENT RECRUITING OFFICES.—

(a) DIGITAL TALENT RECRUITING FOR THE DEPARTMENT OF DEFENSE.—

(1) Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense shall designate a chief digital recruiting officer within the office of the Under Secretary of Defense for Personnel and Readiness to oversee a digital recruiting office to carry out the responsibilities set forth in paragraph (2).

(2) The chief digital recruiting officer shall be responsible for—

(A) identifying Department of Defense needs for specific types of digital talent;

(B) recruiting technologists, in partnership with the military services and defense components, including by attending conferences and career fairs, and actively recruiting on university campuses and from the private sector;

(C) integrating Federal scholarship for service programs into civilian recruiting;

(D) offering recruitment and referral bonuses; and

(E) partnering with human resource teams in the military services and defense components to use direct-hire authorities to accelerate hiring.

(3) The Secretary of Defense shall ensure that the chief digital recruiting officer is provided with personnel and resources sufficient to maintain an office and to carry out the duties set forth in paragraph (2).

(b) DIGITAL TALENT RECRUITING FOR THE INTELLIGENCE COMMUNITY.—

(1) Not later than 270 days after the date of the enactment of this Act, the Director of National Intelligence shall designate a chief digital recruiting officer to oversee a digital recruiting office to carry out the responsibilities set forth in paragraph (2).

(2) The chief digital recruiting officer shall be responsible for—

(A) identifying intelligence community needs for specific types of digital talent;

(B) recruiting technologists, in partnership with components of the intelligence community, by attending conferences and career fairs, and actively recruiting on college campuses;

(C) integrating Federal scholarship for service programs into intelligence community recruiting;

(D) offering recruitment and referral bonuses; and

(E) partnering with human resource teams in the components of the intelligence community to use direct-hire authorities to accelerate hiring.

(3) The Director of National Intelligence shall ensure that the chief digital recruiting officer is provided with personnel and resources sufficient to maintain an office and to carry out the duties set forth in paragraph (2).

(c) DIGITAL TALENT RECRUITING FOR THE DEPARTMENT OF HOMELAND SECURITY.—

(1) Not later than 270 days after the date of the enactment of this Act, the Secretary of Homeland Security shall designate a chief digital recruiting officer to oversee a digital recruiting office to carry out the responsibilities set forth in paragraph (2).

(2) The chief digital recruiting officer shall be responsible for—

(A) identifying Department of Homeland Security needs for specific types of digital talent;

(B) recruiting technologists, in partnership with components of the Department of Homeland Security, by attending conferences and career fairs, and actively recruiting on college campuses;

(C) integrating Federal scholarship for service programs into civilian recruiting;

(D) offering recruitment and referral bonuses; and

(E) partnering with human resource teams in the components of the Department of Homeland Security to use direct-hire authorities to accelerate hiring.

(3) The Secretary of Homeland Security shall ensure that the chief digital recruiting officer is provided with personnel and resources sufficient to maintain an office and to carry out the duties set forth in paragraph (2).

(d) DIGITAL TALENT RECRUITING FOR THE DEPARTMENT OF ENERGY.—

(1) Not later than 270 days after the date of the enactment of this Act, the Secretary of Energy shall designate a chief digital recruiting officer to oversee a digital recruiting office to carry out the responsibilities set forth in paragraph (2).

(2) The chief digital recruiting officer shall be responsible for—

(A) identifying Department of Energy needs for specific types of digital talent;

(B) recruiting technologists, in partnership with Department of Energy programs, by attending conferences and career fairs, and actively recruiting on college campuses;

(C) integrating federal scholarship for service programs into civilian recruiting;

(D) offering recruitment and referral bonuses; and

(E) partnering with human resource teams in Department of Energy programs to use direct-hire authorities to accelerate hiring.

(3) The Secretary of Energy shall ensure that the chief digital recruiting officer is provided with personnel and resources sufficient to maintain an office and to carry out the duties set forth in paragraph (2).

Recommendation 1.11: Establish PPTE program at non-DoD National Security agencies

SEC. __.—PUBLIC-PRIVATE TALENT EXCHANGE FOR NATIONAL SECURITY.—

(a) ESTABLISHMENT OF PUBLIC-PRIVATE TALENT EXCHANGE PROGRAM FOR NATIONAL SECURITY.—

(1) Not later than 180 days after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations to establish a public-private talent exchange program, to be administered at each designated agency, for the purpose of developing and accessing critical skills necessary to address national security needs of the United States.

(2) The program established by this section shall allow for the temporary assignment of an employee of a designated agency to a private-sector organization and for the temporary assignment of an employee of a private-sector organization to address national security needs of the United States. Such assignments shall be made pursuant to agreements among the designated agency involved in the specific assignment, private-sector organization involved in the specific assignment, and the individual to be assigned to the designated agency or to the private-sector organization.

(3) Nothing in this section or regulations implementing this section shall be construed to limit or condition the authority of the Secretary of Defense to provide for a separate public-private talent exchange program pursuant to section 1599g of title 10, United States Code.

(b) AGREEMENT FOR TEMPORARY ASSIGNMENT OF INDIVIDUALS FROM DESIGNATED AGENCIES TO PRIVATE-SECTOR ORGANIZATIONS AND FROM PRIVATE-SECTOR ORGANIZATIONS TO DESIGNATED AGENCIES.—

(1) The Director of the Office of Personnel Management shall develop one or more model agreements to govern the temporary assignment of individuals for the program established under this section. The model agreements may be adapted, in accordance with regulations issued by the Director, by each head of a designated agency.

(2) An agreement for the assignment of an individual from a designated agency to a private-sector organization—

(A) shall require that the employee of the designated agency, upon completion of the assignment, will serve in the designated agency, or elsewhere in the civil service if approved by the head of the designated agency, for a period equal to twice the length of the assignment;

(B) shall provide that if the employee of the designated agency or of the private-sector organization (as the case may be) fails to carry out the agreement, such employee shall be liable to the United States for payment of all expenses of the assignment, unless that failure was for good and sufficient reason, as determined by the head of the designated agency; and

(C) shall contain language ensuring that such employee does not improperly use pre-decisional or draft deliberative information that such employee may be privy to or aware of related to designated agency programing, budgeting, resourcing, acquisition, or procurement for the benefit or advantage of the private-sector organization.

(3) An amount for which an employee is liable under paragraph (2) shall be treated as a debt due the United States.

(4) The head of a designated agency may waive, in whole or in part, collection of a debt described in paragraph (3) based on a determination that the collection would be against equity and good conscience and not in the best interests of the United States, after taking into account any indication of fraud, misrepresentation, fault, or lack of good faith on the part of the employee.

(c) TERMINATION.—An assignment under the program established by this section may, at any time and for any reason, be terminated by the designated agency or the private-sector organization concerned.

(d) LIMITS ON DURATION.—

(1) An assignment under the program established by this section shall be for a period of not less than three months and not more than two years, renewable up to a total of four years. No employee of a designated agency may be assigned under this section for more than a total of four years inclusive of all such assignments.

(2) An assignment under this section may be for a period in excess of two years, but not more than four years, if the head of the designated agency determines that such assignment is necessary to meet critical mission or program requirements.

(e) STATUS OF FEDERAL EMPLOYEES ASSIGNED TO PRIVATE-SECTOR ORGANIZATIONS.—

(1) An employee of a designated agency who is assigned to a private-sector organization under this section shall be considered, during the period of assignment, to be on detail to a regular work assignment in the designated agency for all purposes. The written agreement established under subsection (b)(1) shall address the specific terms and conditions related to the employee's continued status as a Federal employee.

(2) In establishing a temporary assignment of an employee of the designated agency to a private-sector organization, the head of the designated agency shall—

(A) ensure that the normal duties and functions of such employee can be reasonably performed by other employees of the designated agency without the permanent transfer or reassignment of other personnel of the designated agency;

(B) ensure that the normal duties and functions of such employees are not, as a result of and during the course of such temporary assignment, performed or augmented by contractor personnel; and

(C) certify that the temporary assignment of such employee shall not have an adverse or negative impact on mission attainment, national security, or organizational capabilities associated with the assignment.

(f) TERMS AND CONDITIONS FOR PRIVATE SECTOR EMPLOYEES ASSIGNED TO DESIGNATED AGENCIES.—An employee of a private-sector organization who is assigned to a designated agency under this section—

(1) shall continue to receive pay and benefits from the private-sector organization from which such employee is assigned and shall not receive pay or benefits from the Federal Government, except as provided in paragraph (2);

(2) is deemed to be an employee of the designated agency for the purposes of—

(A) chapters 73 and 81 of title 5, United States Code;

(B) sections 201, 203, 205, 207, 208, 209, 603, 606, 607, 643, 654, 1905, and 1913 of title 18, United States Code;

(C) sections 1343, 1344, and 1349(b) of title 31, United States Code;

(D) the Federal Tort Claims Act and any other Federal tort liability statute;

(E) the Ethics in Government Act of 1978; and

(F) chapter 21 of title 41, United States Code;

(3) shall not have access to any trade secrets or to any other nonpublic information which is of commercial value to the private-sector organization from which such employee is assigned;

(4) may not perform work that is considered inherently governmental in nature; and

(5) may not be used to circumvent the requirements of Office of Management and Budget Circular A-76 or to circumvent any limitation or restriction on the size of the workforce of the designated agency.

(g) PROHIBITION AGAINST CHARGING CERTAIN COSTS TO THE FEDERAL GOVERNMENT.—A private-sector organization may not charge any agency of the Federal Government, as direct or indirect costs under a Federal contract, the costs of pay or benefits paid by the organization to an employee assigned to a designated agency under this section for the period of the assignment.

(h) CONSIDERATIONS.—In carrying out this section, the heads of designated agencies—

(1) shall ensure that, of the assignments made under this section each year, at least 20 percent are from small business concerns (as defined by section 3(a)(2) of the Small Business Act);

(2) shall take into consideration the question of how assignments under this section might best be used to help meet the needs of the designated agency with respect to the training of employees and accessing critical national security-related skills; and

(3) shall take into consideration, where applicable, areas of particular private sector expertise relevant to the national security needs of the United States, such as cybersecurity and artificial intelligence.

(i) CONFLICTS OF INTEREST.—A private-sector organization that is temporarily assigned a member of the acquisition workforce under this section shall not be considered to have a conflict of interest with the designated agency solely because of participation in the program established under this section.

(j) DEFINITIONS.—In this section:

(1) HEADS OF DESIGNATED AGENCIES.—The term “heads of designated agencies” means the Secretary of State, the Secretary of Homeland Security, the Secretary of Energy, the Secretary of Commerce, and the Secretary of the Treasury.

(2) DESIGNATED AGENCIES.—The term "designated agencies" means the Department of State, the Department of Homeland Security, the Department of Energy, the Department of Commerce, and the Department of the Treasury.

Recommendation 1.12: Create New Career Fields

SEC. ___.—MILITARY CAREER FIELDS FOR SOFTWARE DEVELOPMENT, DATA SCIENCE, AND ARTIFICIAL INTELLIGENCE.—Section 230 of the National Defense Authorization Act for Fiscal Year 2020 is amended by adding the following new subsection:

"(d) Not later than 270 days after the date of the enactment of this subsection, the Chief of Staff of the Army, the Chief of Naval Operations, the Chief of Staff of the Air Force, and the Commandant of the Marine Corps (collectively, the Service Chiefs) shall each establish new military career fields for software development, data science, and artificial intelligence that are open to commissioned officers, enlisted personnel and, as appropriate, warrant officers. The Service Chiefs shall utilize the authority provided in sections 605 and 649a to 649k of title 10, United States Code to ensure that military personnel in these career fields who choose to specialize and focus on technical skill sets rather than pursue leadership positions are not required to move outside their specialties or into management positions to continue to promote."

Recommendation 1.13: Create ASI, AQD, AMOS, and SEI for Topics Related to AI

SEC. ___.—IDENTIFIERS FOR CRITICAL DIGITAL SKILLS IN THE MILITARY.—Not later than 270 days after the date of the enactment of this Act, the Chief of Staff of the Army, the Chief of Naval Operations, the Chief of Staff of the Air Force, and the Commandant of the Marine Corps (collectively, the Service Chiefs) shall establish Additional Skill Identifiers (ASI), Additional Qualification Designations (AQD), Additional Military Occupational Specialty (AMOS), or Special Experience Identifiers (SEI), as appropriate, with associated instructional courses and certification requirements to recognize skills gained in the areas of mission engineering, data engineering, safety and responsible artificial intelligence engineering, and artificial intelligence hardware technicians.

Recommendation 1.14: Integrating Digital Skill Sets and Computational Thinking into Military Junior Leader Education

SEC. ___.—INTEGRATING DIGITAL SKILL SETS AND COMPUTATIONAL THINKING INTO MILITARY JUNIOR LEADER EDUCATION.—Not later than 270 days after the date of the enactment of this Act, the Chief of Staff of the Army, the Chief of Naval Operations, the Chief of Staff of the Air Force, and the Commandant of the Marine Corps (collectively, the Service Chiefs) shall expand the curriculum for military junior leader education to incorporate appropriate training material related to problem definition and curation, a conceptual understanding of the artificial intelligence lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making. Whenever possible, the new training and education should include the use of existing artificial intelligence-enabled systems and tools.

Recommendation 1.15: Integrating Digital Skill Sets and Computational Thinking into Civilian Junior Leader Education

SEC. ___.—ASSESSMENT OF APPROACHES TO INTEGRATING DIGITAL SKILL SETS AND COMPUTATIONAL THINKING INTO CIVILIAN JUNIOR LEADER EDUCATION.—

(a) REPORTS REQUIRED.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense, the Secretary of Energy, the Secretary of Homeland Security, and the Director of National Intelligence shall each report to Congress on the integration of digital skill sets and computational thinking into civilian junior leader education in their respective departments or communities.

(b) MATTERS TO BE ADDRESSED.—Each report required by subsection (a) shall provide, at a minimum, the following:

(1) An assessment identifying the components of the workforce of the relevant department or community whose roles involve or will involve supporting or using artificial intelligence-enabled systems;

(2) An assessment of methods of ensuring that civilian junior leaders in such workforce components receive appropriate training regarding problem definition and curation, a conceptual understanding of the artificial intelligence lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making; and

(3) An assessment of positions with the relevant department or community for which position descriptions should be modified to address artificial intelligence-related tasks.

Recommendation 1.16: Integrate Emerging Technologies Material into Courses for Officers as part of Service-level Professional Military Education

SEC. ___.—INTEGRATION OF MATERIAL ON EMERGING TECHNOLOGIES INTO PROFESSIONAL MILITARY EDUCATION.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense, in consultation with the Joint Chiefs of Staff, shall ensure that the curriculum for professional military education is revised in each of the military services to incorporate periodic courses on militarily significant emerging technologies that increasingly build the knowledge base, vocabulary, and skills necessary to intelligently analyze and utilize emerging technologies in the tactical, operational, and strategic levels of warfighting and warfighting support.

Recommendation 1.17: Require A Short Course for General and Flag Officers and SES Leadership Focused on Emerging Technologies

SEC. ___.—SHORT COURSE ON EMERGING TECHNOLOGIES FOR SENIOR CIVILIAN AND MILITARY LEADERS.—

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall establish a short course on emerging technologies for general and flag officers and senior executive-level civilian leaders. The short course shall be taught on an iterative, two-year cycle and shall address the most recent, most relevant technologies and how these technologies may be applied to military and business outcomes in the Department of Defense.

(b) THROUGHPUT OBJECTIVES.—In assessing participation in the short course authorized by subsection (a), the Secretary of Defense shall ensure that:

(1) In the first year that the course is offered, no fewer than twenty percent of general flag officers and senior executive-level civilian leaders are certified as having passed the short course required by subsection (a); and

(2) In each subsequent year, an additional ten percent of general flag officers and senior executive-level civilian leaders are certified as having passed such course, until such time as eighty percent of such officers and leaders are so certified.

Recommendation 1.18: Create Emerging Technology Coded Billets Within the Department of Defense

SEC. ___.—EMERGING TECHNOLOGY-CODED BILLETS WITHIN THE DEPARTMENT OF DEFENSE.—

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall ensure that the military services—

(1) code appropriate billets to be filled by emerging technology-qualified officers; and

(2) develop a process for officers to become emerging technology-qualified.

(b) APPROPRIATE POSITIONS.—Emerging technology-coded positions may include, as appropriate—

(1) positions responsible for assisting with acquisition of emerging technologies;

(2) positions responsible for helping integrate technology into field units;

(3) positions responsible for developing organizational and operational concepts;

(4) positions responsible for developing training and education plans; and

(5) leadership positions at the operational and tactical levels within the military services.

(c) QUALIFICATION PROCESS.—The process for qualifying officers for emerging technology-coded billets shall be modeled on a streamlined version of the joint qualification process and may include credit for serving in emerging technology focused fellowships, emerging technology focused talent exchanges, emerging technology focused positions within government, and educational courses focused on emerging technologies.

Recommendation 1.19: Require Short Courses for Policy Personnel with AI-Related Portfolios

SEC. ___.—SHORT COURSE ON ARTIFICIAL INTELLIGENCE FOR POLICY PERSONNEL WITH ARTIFICIAL INTELLIGENCE-RELATED PORTFOLIOS.—

(a) IDENTIFICATION OF POLICY PERSONNEL.—Not later than one year after the date of the enactment of this Act, the Secretary of State, the Secretary of Defense, the Secretary of Commerce, the Secretary of Energy, the Secretary of Homeland Security, and the Director of National Intelligence shall each identify policy experts within their respective departments or communities whose portfolios affect or will be affected by artificial intelligence.

(b) ESTABLISHMENT OF SHORT COURSE.—Not later than one year after the date of the enactment of this Act, the Secretary of State, the Secretary of Defense, the Secretary of Commerce, the Secretary of Energy, the Secretary of Homeland Security, and the Director of National Intelligence shall each establish a short course on artificial intelligence, its capabilities, and related policy topics for the officials identified pursuant to subsection (a).

(c) THROUGHPUT OBJECTIVES.—It shall be the objective of the Federal Government to ensure that no fewer than 50 percent of the policy experts identified pursuant to subsection (a) in each of the covered departments or communities successfully complete a short course established under subsection (b) within two years of the date of the enactment of this Act.

Recommendation 1.20: Require Emerging Technology Training for Specific Acquisition Functional Areas

SEC. ___.—UPDATED EMERGING TECHNOLOGY TRAINING FOR SPECIFIC ACQUISITION FUNCTIONAL AREAS.—

(a) ANNUAL ASSESSMENT.—The President of the Defense Acquisition University shall conduct an annual assessment of the emerging technology education needs of the acquisition workforce in partnership with the Under Secretary of Defense for Research and Engineering.

(b) UPDATED TRAINING PROGRAM.—No later than 180 days after the completion of each annual assessment conducted pursuant to subsection (a), the President of the Defense Acquisition University shall update the curriculum of the University to design and offer functional area specific courses on emerging technologies to meet the needs identified by such annual assessment.

TAB 5 — Legislative Language

Recommendation 7: Congress should establish a Small Business Administration grant program to enable small- and medium-sized U.S. AI companies to participate in international standardization efforts.

SEC. __.—SUPPORT FOR INDUSTRY PARTICIPATION IN INTERNATIONAL STANDARDS ORGANIZATIONS.—

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Small Business Administration shall establish a program to support participation by small business concerns in meetings and proceedings of international standards organizations in the development of voluntary technical standards.

(b) GRANTS AUTHORIZED.—In carrying out the program authorized by subsection (a), the Administrator shall award competitive, merit-reviewed grants, to small business concerns to cover the reasonable costs, up to a specified ceiling, of participation of employees of such businesses in meetings and proceedings of international standards organizations. Participation may include regularly attending meetings, contributing expertise and research, proposing new work items, volunteering for leadership roles such as convenors and editors, and being early adopters of emerging standards. Recipients of awards under this subsection shall not be required to provide a matching contribution.

(c) AWARD CRITERIA.—The Administrator may provide under this section a grant award to covered entities that:

(1) demonstrate deep technical expertise in key emerging technologies, including Artificial Intelligence and related technologies;

(2) commit personnel with such expertise to regular participation in international bodies responsible for setting standards for such technologies over the period of the grant; and

(3) agree to participate in efforts to coordinate between the U.S. government and industry to ensure protection of national security interests in the setting of international standards.

(d) EVALUATION.—In issuing awards under this section, the Administrator shall coordinate with the Director of the National Institute of Standards and Technology who shall provide support in the assessment of technical expertise in emerging technologies and standards setting needs.

(e) DEFINITIONS.—In this section:

(1) ADMINISTRATOR.—The term "Administrator" means the Administrator of the Small Business Administration.

(2) COVERED ENTITY.—The term "covered entity" means a small business concern that is incorporated in and maintains a primary place of business in the United States.

(3) SMALL BUSINESS CONCERN.—The term "small business concern" has the same definition as set out in section 632 of title 15, United States Code.

(f) AUTHORIZATION OF APPROPRIATION.—There is authorized to be appropriated for fiscal year 2022 and each fiscal year thereafter $1 million to carry out the program authorized in this section.

APPENDIX II – Third Quarter Recommendations Funding Table

Category	Recommendation & Description		Cabinet Departments and Major Agencies	Amount*
Tab 1: Strengthening the Triangular Alliance for AI R&D	1.................	Create an AI Innovator Award Program to Invest in Top Talent	National Science Foundation	$125 million
	2.................	Invest in Research Teams Pursuing Transformative Ideas in AI	National Science Foundation	$50-250 million**
	4.................	Support AI Dataset Curation and Maintenance	Department of Energy	$25 million
	5.................	Launch an AI Research Challenge	Department of Defense USD(R&E) - DARPA	$75 million
	8.................	Launch an AI Catalyst Initiative	Department of Defense USD(R&E)	$100-250 million
Tab 2: Applying AI for National Security Missions	1.................	Additional funding for USD(R&E) SIAC technology scouting	Department of Defense USD(R&E)	$10 million
	3.................	Dedicated USD(R&E) fund to mature, prototype and transition AI technologies	Department of Defense USD(R&E)	$200-250 million
	4.................	Dedicated ODNI Director S&T fund to identify and invest in AI applications	Office of the Director of National Intelligence	$200-250 million
Tab 3: Train and Recruit AI Talent	1.1..............	Support Army AI Task Force's AI and Data Science Workforce Initiative	Department of Defense Department of the Army	$5 million for FY22 and $6 million for FY23
	1.3..............	Support the Air Force Digital University	Department of Defense Department of the Air Force	$10 million
	1.4..............	Support the Air Force Computer Language Initiative	Department of Defense Department of the Air Force	$10 million
	1.5..............	Support the U.S. Air Force/Massachusetts Institute of Technology (MIT) AI Accelerator	Department of Defense Department of the Air Force	$15 million

	1.8.............	Enact the Science, Technology, Engineering, and Mathematics (STEM) Corps Proposal.	Department of Defense	$5 million
	2.1.............	National Defense Education Act II	Department of Education	$8.05 billion
	2.1.............	National Defense Education Act II	National Science Foundation	$175 million
	2.2.............	Mid-Career Faculty Fellowships	National Science Foundation	$15 million
	2.3.............	Support Creation of Pilot Program for Artificial Intelligence Technology and Education Improvements for Community Colleges.	National Science Foundation	$30 million
	2.4.............	Creation of AI-Specific Government Internships.	Department of Education	$2 million
	2.5.............	Increase Incentives for Public-Private Job Reskilling Training	Department of Education	$2.7 billion
	2.7.............	Create a National Microelectronics Scholar Program	Department of Defense USD(A&S)	$60 million
Tab 5: Marshal Global AI Cooperation	6................	Create interagency AI Standards team to support NIST AI Standards Coordinator	(1) Department of Commerce National Institute of Science and Technology; (2) Department of Defense Joint Artificial Intelligence Center; (3) Department of State Under Secretary for Economic Growth, Energy and Environment; (4) Office of the Director of National Intelligence; (5) Department of Homeland Security Science and Technology Directorate; and, (6) Department of Energy Artificial Intelligence & Technology Office	$3 million
	7................	Small Business Administration grant program for international standardization	Small Business Administration	$1 million

** Unless otherwise noted funding for Fiscal Year 2022.*

*** Tab 1, Recommendation 2, recommends the following appropriations amounts $50 million for Fiscal Year 2022, $100 million for Fiscal Year 2023, $150 for Fiscal Year 2024, $200 for Fiscal Year 2025, $250 million for Fiscal Years 2026, 2027, and 2028.*

NATIONAL
SECURITY
COMMISSION
ON ARTIFICIAL
INTELLIGENCE