# A HOLISTIC APPROACH TO PROTECTING NATIONAL SECURITY: INTEGRATING INTELLIGENCE AND RISK MANAGEMENT TO REDUCE INSIDER THREATS

by
George Stephen Hyek

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts

Baltimore, Maryland
December 2020

# ABSTRACT

Reviewed by Thomas Stanton and Anthony Lang, this thesis explores the important question of how a combination of security intelligence and risk management could be used to address insider threats and their impact on national security. As the thesis documents, insiders threaten not only the wellbeing of employees and facilities, but also the confidentiality and integrity of sensitive information, which could be used by foreign adversaries of the United States. The first chapter recommends more systematic integration of intelligence information into security programs. The second chapter explores the role of risk management, and especially Enterprise Risk Management, in improving the effectiveness of federal security programs and organizations. The third chapter focuses directly on the problem of insider threats. It highlights the remarkable number of ways that insiders such as Edward Snowden displayed warning signs of the danger they posed to national security, long before the damage they caused occurred.

It was discovered that analyzing current threat information, which makes it intelligence, enables security programs to allocate resources and deploy countermeasures more appropriately. The intelligence findings enable risk management, which is the ongoing process federal organizations use to determine how they will respond to threats. Organizations that fail to understand their threat, and subsequently impose risk-driven countermeasures, are likely to suffer consequences from attacks – many of which come from insider threats. Insiders acting against federal organizations stand to damage national security by harming people they work with, revealing defense secrets, and/or weakening international relations. The potential damage to national security can be mitigated using the holistic approach outlined throughout this thesis.

# Contents

# Thesis Introduction

Insider threats consistently prove to be an evolving challenge for U.S. national security. The concept of a trusted employee using their privileged access to classified secrets for harm is difficult to fathom for many of the dedicated professionals in public service. Yet, the threat persists through both the cyber and physical domains. The rapid development of technology coupled with any insider's legitimate access makes them exceptionally difficult to discover. To effectively mitigate the risk posed by insider threats, risk management and intelligence analysis must be intertwined in the foundation federal security programs are built upon. Security programs charged with protecting defense organizations that fail to integrate those ancillary considerations jeopardize national security, with consequences ranging between lost American lives, global economic implications, and geopolitical standing. This thesis examines insider threats and federal security programs in the broader context of utilizing security intelligence and risk management for improved protection and safeguarding of national security.

The first chapter explores how federal security programs benefit from integrating with intelligence analysis, creating a subdiscipline known as security intelligence. It was found that analyzing current threat information, which makes it intelligence, enables security programs to allocate resources and deploy countermeasures more effectively. However, varying authorities between executive departments creates collection challenges for organizations within the Department of Defense (DoD). The Departments of Justice and Homeland Security are authorized to passively collect intelligence on U.S. persons, but the DoD is not due to their wartime mission, making their focus more on foreign intelligence targets. This dichotomy of authorities makes interagency cooperation imperative for defending against the predominately domestic nature of insider threats to national security. Yet, case studies illustrate how each department's varying mission puts them at odds for sharing threat information; the undulation between prosecution and collection priorities rages on between executive departments.

The second chapter explores how risk management works with federal security programs. Enterprise Risk Management is a term often used in organizations for financial decision making, but how it pertains to security operations and program management was the focus. The process of analyzing threats, vulnerabilities, and potential impact to determine overall 'risk' is directly applicable and necessary for security programs to be effective. Exploratory research determined there are many executive mandates that require federal organizations to implement risk management practices throughout their workforces. Yet, there is little information on its specific application in daily security practices, making it seem unlikely that individual security officers are aware of the larger risk management strategy. This is an area where additional research may yield more detailed discoveries and opportunities for improvement; albeit, the concept proves how security programs must remain flexible and can benefit from implementing the various stages of risk management to adapt their activities to the assessed needs.

The final chapter is a deep dive into what insider threats are and how they impact national security, before tying the entire thesis portfolio together by introducing risk management and security intelligence into the scenario. The research question of 'how insider threats impact national security' drove the chapter's research. It begins by first framing what an insider threat really is, using nationally accepted definitions. After providing a solid foundation and definition of what an insider threat really means, exactly how they stand to damage national security is illustrated using real world ramifications as examples. Most notably, insiders can cost American lives by disclosing secrets to U.S. adversaries pertaining to the defenses they may encounter, the sources and methods used to collect intelligence, and sabotaging international relations.

The case studies of Nidal Hasan and Edward Snowden are used to illustrate the nature and varying consequences associated with insider threats – violence and espionage. The Snowden case study is then used to tie the entire portfolio together by illuminating how his attack on national security may have been mitigated with better risk management and intelligence. There were many early indications and warning signs that Snowden was a risk, who could eventually manifest into an insider threat. Yet, many were dismissed and not investigated to the extent that could have prevented his attack and the subsequent damage he caused, illustrating security failures. As a result, risk management changed dramatically at the National Security Agency (NSA) and that evidence is presented.

The author of this thesis works in the security field and used firsthand observations with empirical analysis to guide the research. Exploratory research was the primary method for determining the relationships between risk management, intelligence, and analysis. However, four expert interviews were also conducted with members responsible for security within the intelligence community and a subject matter expert in risk management from Carnegie Mellon University. The sources used in this thesis ranged from primary to tertiary literature. The primary literature proved to be invaluable case studies conducted by the agencies that responded to some of the tragic events. Furthermore, the National Security Agency's (NSA) Chief Risk Officer, who was appointed after the Snowden attack, was interviewed several times, and provided significant insight to the process they went through. Additionally, guidelines, manuals, executive orders, and doctrines were used as primary sources.

Some necessary research was impossible to acquire given the nature of it being classified and this being an unclassified process. For example, there was a report generated by Congress that literally outlined the exact damage Snowden's attack had on national security, which was one of the main points of the thesis. Unfortunately, that report was classified as Top Secret and therefore could not be found on the open internet or be used in this study. As a result, redacted versions released through the Freedom of Information Act and other unclassified documents were used to piece together the likely impact. There was also a lack of strong sources detailing the specifics of risk management influences every day security practices. This may be for good reason – they do not want to publish everyday security practices that would give an advantage to adversaries seeking to thwart them. Yet, the tactical effects of how risk management is used by security officers is still unclear; so, this thesis speaks more to the strategic benefits.

Security programs are complex as they include responsibilities in both the physical and information domains. Yet they differ between the federal and private sectors as those organizations are typically revenue oriented and the government is not. Plus, the threat landscape differs by the motivations of the attackers. Attackers in the private sector often share their victim's motivation, which is money. Whereas, those who attack the government are more likely motivated by political or strategic incentives, such as intelligence collection or sabotaging U.S. interests. Regardless, of the sector or attackers' motivations, security programs are tasked with protecting their organization's people, places, and information; an increasingly difficult task today with the advancements in cyber. Yet, security is always an overhead expense and, therefore, under constant scrutiny, making efficacy extremely important.

Security programs in federal organizations are often broken down into three categories: information (aka cyber), physical, and personnel. Information security is responsible for safeguarding the organization’s information, be it written or printed on physical material or in cyberspace. Physical security is often the most recognizable; it often includes the organization’s uniformed security officers, security systems, and access control countermeasures. Personnel security is often less noticeable to the untrained eye, but includes all the administrative tasks associated with processing and granting security clearances. Personnel security in the federal sector is crucial as there are varying degrees of ‘need to know,’ which determines clearance levels, security caveats, and prevents accidental ‘spillage’ incidents.

Given the three distinct branches of security that make up federal security programs, there are unique personnel working in each, different leadership, and different goals, which ultimately creates a silo effect. The different cultures throughout the branches impacts the overall effectiveness as there is often a lack of understanding amongst those tasked with achieving the same goal. This is important because attackers have recognized the seams between departments and have recently began exploiting the subsequent vulnerabilities. Many of these attacks are known as ‘social engineering,’ which a finely tuned security program should be capable of preventing. Communication between the various security programs and senior leadership is imperative, but the security program’s strategy must ultimately be rooted in risk management.

How can a security program accurately assign, train, or equip its personnel without having a thorough understanding of the threats it may face? The answer is that it cannot; it needs intelligence collection and analysis to accurately capture the threat data. Once the threat data is understood, risk management can be used to accurately allocate resources according to the unique needs. First, senior leadership provides the organization’s risk appetite, which serves as the benchmark for practitioners to plan against. The analysis of the threat data combined with internal vulnerabilities and the impact of a breach is what determines the overall risk. When the actual risk expands beyond the risk appetite, the security program is meant to reduce the risk to an acceptable level through its many safeguards and countermeasures.

Seeing how intelligence enables risk management and risk management drives security operations, the practical application of this model should be extremely important to senior leaders. Once established, the cycle is fluid and changes based on the threat landscape, which intelligence will indicate. Then risk management can determine the correct balance of safeguards with acceptable loss and security can execute accordingly. Since the security programs discussed are tasked with protecting the organizations that are charged with protecting America, ensuring they operate effectively is paramount to national security. Afterall, a poorly handled security event, or oversight, could lead to a situation such as Edward Snowden, Nidal Hasan, or Aaron Alexis. Yet, a failure of security calls into question the effectiveness of the risk management process as well because it is possible the security program was not resourced properly or failed to capture requisite intelligence.

## Chapter 1: Security Intelligence

Achieving a state of safety and security is the second level of Maslow's hierarchy of basic needs. It is human instinct to constantly limit risk and attain a state of security, which is to be free from danger or threat. Yet, it is the nature of virtually any threat to adapt and overcome obstacles preventing it from achieving its objectives. Federal site security programs are susceptible to attacks in both the physical and information domains, which jeopardizes national security by impacting their operations. Currently, federal approaches to security are decentralized, relying on disconnected organizations and departments to prevent and see any incident through. Threat actors can exploit this seam in security coverage by using a blend of physical and cyber activities to execute their attacks in each domain. Integrating intelligence collection and analysis into security plans may eliminate the vulnerabilities and security oversights that a non-holistic security program would miss, while also decreasing response times.

The constant undulation between security and risk drastically evolved in the 1980s with the invention of the World Wide Web. Unchecked technology that evolved faster than the average citizen or employees (the entities needing protection) could mitigate. There is a lack of awareness and a sense that the average internet user is a passive recipient of all the internet has to offer, negative and positive, creating a new set of threats and subsequent risk. For this reason, it is more important than ever to design cost effective security programs that account for more than the traditional 'guards, gates, and guns' as seen in most disparate security programs used by the federal government. Security programs must protect against numerous physical threats, like active shooters, whilst also maintaining the ability to prevent adversaries from obtaining sensitive classified information or sabotaging operations in the cyber domain. A security program's countermeasures should be determined by a robust risk management cycle, which benefits if driven by intelligence analysis. Detailing the advantages of fusing intelligence and security into one holistic security program federal agencies is the objective of this thesis.

As the threat landscape expanded in breadth and depth, many policies changed and standards were established by the highest offices in the federal government to compensate; examples are changes in national policy by every administration since President Clinton, the minimum standards set by the National Insider Threat Task Force (NITTF), and executive orders 10450, 12333 and 12968. However, the seam between physical security and cyber security continues to be a vulnerability due to cyber security's relatively infantile stage of life (compared to physical) and the continued trial and error of fusing the two disciplines into a harmonious security program.

Most security programs are designed with the assumption that a dedicated attacker will not be thwarted by a single layer of security, so numerous protective countermeasures are implemented to secure the innermost assets of the facility. However, the funding and specific countermeasures are commensurate of the risk levels, which can only be determined through intelligence collection and analysis. Risk-informed analysis enables the agency to allocate appropriate funding and resources to meet their needs. The fusion of both creates a symbiotic program capable of offering better protection and reducing costs.

Effective security is required at any federal agency and cleared defense contractor (CDC) with federal equities. It also accounts for the added risk of Sensitive Compartmented Information Facilities (SCIFs), where classified information is processed. The agencies who use intelligence to drive security will be referred to as ‘customers’ because understanding that security is a customer-centric function is imperative to its success. The difference between this kind of customer service and the meaning in a traditional sense is that it is inward facing and is a mentality, not just a business practice used to garner revenue.

Based on the current vulnerabilities of the techno-landscape, best practices implementing holistic security programs should be the norm for industry protection throughout the federal government; however, this is not the case. Countless attacks and attempts to collect information on federal and CDC customers prove the need for evolution in security practices. Discovered attacks encompass a wide array of threats, from physical breaches to remote hacking. Some intend to steal valuable classified information, while others seek to achieve loss of life. A holistic security program will minimize risk by accounting for all threats and better preparing the organization to deal with any attack or breach in the most timely and pragmatic way possible.

## History of Security Failures

Timothy McVeigh, a U.S. Army Veteran, was responsible for killing 168 people in the Oklahoma City bombing against the Murrah Federal Building in 1995. His anti-government ideology served as motivation for his attack; his hatred was exacerbated by the Waco siege and the Ruby Ridge standoff.[1] After a short reconnaissance of targets, McVeigh recognized a vulnerability in the Federal Building's access control security that would enable him to drive a vehicle born improvised explosive device close enough to the building that a detonation would create mass causalities. Since McVeigh was not an insider, his presence at the federal facility was an indicator of malign intent and is likely the reason he could not get the bomb inside the internal parking garage, which would have caused additional damage. Yet, his plan worked as the explosion seared off approximately a third of the building, killing men, women, and children inside.

If the Murrah building's security was more effectively planned and managed, McVeigh would not have been able to drive the truck close enough to create such a catastrophe. It is likely that if the threat landscape was ever assessed for the building, it was a static assessment and not continually considered, which is problematic because threats evolve with real world events, like Ruby Ridge and Waco. Additionally, who made the decision that entrance bollards were not worth the investment or necessary? There is no information on that logic blunder, but the conversation may have only occurred by the original building architects and the property

[1] Gumbel, A. Oklahoma City bombing: 20 years later, key questions remain unanswered. April 13, 2015

management personnel, certainly not security or risk management experts. A fused approach to security would have included ongoing intelligence analysis of the threat landscape, which would have likely prompted the need for additional countermeasures such as bollards. This attack also set a new benchmark for risk analysis on federal facilities and created lessons learned that prompted the FBI to create 56 standalone field offices.

An example of an attack by a foreign intelligence entity was Ana Montes, a Cuban spy, who was driven by different intentions than McVeigh. Montes was recruited to spy for the Cuban government in 1984 while she was working for the Department of Justice, but at the time she did not have a job that provided access to useful intelligence.[2] Shortly after being recruited, she applied to and was accepted for a job with the Defense Intelligence Agency (DIA), where she worked at the U.S. Southern Command in Florida. Her work in the Intelligence Directorate (J2) provided regular access to vast amounts of intelligence that she passed covertly to her Cuban handlers. She was also able to influence the U.S. Intelligence Community's efforts and findings against Cuba during her time working for them, which is a national security crime known as sabotage. Montes was eventually caught and sentenced for her crimes, but grave damage had already occurred due to her ability to steal classified information and pass it on to a foreign adversary while remaining undetected for so long. Despite many indicators of her activities, Montes was also able to pass the DIA's polygraph through specialized techniques she was taught by her Cuban handlers; exemplifying the value in applying intelligence to the security programs tasked with preventing such deception.

Robert Hanssen, an FBI agent, caused one of the worst intelligence disasters in history by providing the KGB classified information from within throughout the cold war. While remaining

[2] FBI. Ana Montes: Cuban Spy. N.d.

anonymous the entire time he spied for the Russians, Hanssen's efforts caused the execution of numerous KGB assets working for the FBI. Additionally, he informed the Russians of the FBI's collection efforts on the Soviet Embassy in Washington, which cost millions of dollars. Hanssen was regarded as only a mediocre Agent throughout his employment at the FBI and was known to have poor social skills. During his time as an FBI agent, he was never expected of being a spy, rarely encountered security checks, never took a polygraph, and was never asked to submit a financial disclosure statement, which equated to numerous security failures.[3]

At the same time Hanssen was spying, Aldrich Ames was also serving as a double agent for the KGB. Ames worked for the CIA for 31 years in counterintelligence, which is the discipline of intelligence meant to prevent foreign espionage. His work was also focused on Soviet counterintelligence, most notably the KGB and GRU, which is who recruited him to betray his country. Ames was a heavy drinker of alcohol and had marriage problems. During an assignment in Mexico, Ames had at least three extramarital affairs, one of which was with a CIA informant. Romantic affiliations with confidential informants are strictly forbidden by CIA policy, but he kept it a secret. He eventually divorced his wife and incurred a significant financial hardship as a result of their split. It is suspected that Ames began spying for the Russians as a result of his financial troubles, yet all the indicators of the potential were present long before given his risky behavior and poor moral code of conduct.[4] Even though he worked in counterintelligence, a holistic security program would have ensured he was investigated solely based on the many indicators he displayed.

[3] Office of the Inspector General. A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen. (2003, August 14).

[4] Department of State. An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence. (1994, November 01).

In recent history, Edward Snowden achieved notoriety for breaching intelligence oversight by releasing hundreds of thousands to potentially a million secret documents to the global media. Unfortunately, his betrayal damaged U.S. relations with many foreign allies and compromised an undisclosed amount of intelligence operations, costing the U.S. taxpayers and Intelligence Community more than it helped. His rapidly changing ideology, while still employed, was a strong indicator of his eventual actions, yet it was not investigated and the damage was inevitable. Snowden was granted administrative privileges on the NSA's network, which enabled him to view any file without restriction or suspicion. Additionally, there were few, if any, internal audits conducted of who viewed what and the antiquated IT systems allowed him to use thumb drives to steal the data he wanted. While most employees are strictly forbidden to use thumb drives, or any portable electronic devices (PEDs), his administrator status provided him plausible deniability because he could have claimed he was using a thumb drive for a legitimate purpose as part of his responsibilities.[5]

Snowden was a valued employee during his tenure, but became a dangerous insider threat who weakened national security as a result of his betrayal. However, a potentially even more deadly threat was Harold Martin III, who was also a contractor at NSA and stole approximately 50 terabytes of NSA's highly classified information and cyber weapons.[6] Martin differed from Snowden because he intended to sell his stolen property on the dark web to an organization such as the Shadow Brokers, who have released NSA's stolen cyber weapons in the past. The Shadow Brokers are an anonymous organization, or individual, who seemingly exists only to sell top secret cyber weapons and exploits that cybercriminals may use to hack banks, government networks, or even give an advantage to a competing government. Since the Shadow Brokers

[5] Cole, M., & Esposito, R. How Snowden did it. (2013, August 23).

[6] Farivar, C. Feds seized 50TB of data from NSA contractor suspected of theft. (2016, October 20).

seem to favor attacking the NSA, it is possible they have someone employed at the NSA who provides expert insight.

A similar cyber-attack occurred against the FBI in April 2019. Attackers hacked over 1,000 websites to steal information off FBI servers. The data they gathered is sensitive information regarding personal details about federal government employees and cases. The information was posted for sale on the dark web.[7] This attack places everyone who had information stolen at grave risk given the type of people or organizations who would be interested in buying that sort of information. Section III of the DOJ's Order 0904 indicates negligence on the FBI's network security personnel since the attacks were made possible due to untimely security upgrades.[8]

While it is unclear, or not public knowledge, who is behind the FBI attack, it was most likely an organization like the Shadow brokers and not state sponsored. However, other cyber threat actors include nation states, such as Iran, China, and Russia. The Russians are widely believed to have conducted cyber-attacks during the 2016 Presidential election, but more sophisticated attacks constantly occur to undermine the U.S.' national security efforts. All malicious cyber actors are believed to pose a significant threat to the U.S., based on the National Security Strategy of 2017. The strategic document even includes cyber-space when discussing the importance of securing borders, which proves the severity and breadth of the threat. Securing the borders, or perimeter, of a potential target is essential in any security plan and is the first step in the holistic security program.

[7] Whittaker, Z. Hackers publish personal data on thousands of US police officers and federal agents – TechCrunch. (2019, April 13).

[8] Department of Justice Order Cyber Security Program, 0904. (2016).

# Intelligence Drives Security Operations

Security programs are most effective when the customer fully understands their environment and the potential threats through enhanced situational awareness. If a customer has no threat, why would they need security? A correct understanding of threats leads to accurate risk analysis, which enables decision-makers to allocate resources and adjust the security posture accordingly. The best way to articulate a threat landscape is through security intelligence, which uses a combination of all source analysis and counterintelligence operations. Security intelligence is the first element of the holistic security program as it is used to communicate useful threat data, both internal and external to the organization. It is defined by the Dictionary of Military and Associated Terms, 2005, as "intelligence on the identity, capability, and intentions of hostile organizations or individuals who are or may be engaged in espionage, sabotage, or terrorism." Security intelligence differs slightly than common intelligence used for national security. The Central Intelligence Agency defines Intelligence analysis as "the application of individual and collective cognitive methods to weigh data and test hypotheses within a secret socio-cultural context."[9]

The ultimate objective of all intelligence should always be security. Yet, there is a distinguishable difference in the way it is conducted by security programs or for national security purposes. For national security, international intelligence operations have tactical, operational, and strategic benefits, meant for a vast array of recipients ranging from Soldiers in a war zone to the President of the United States. National intelligence also includes powerful information collection assets that are owned and tasked by many different Intelligence / Combat Support Agencies (CSA), all representing a primary intelligence discipline. Before national level

[9] Central Intelligence Agency Library. (2008, June 28).

intelligence products are published, they undergo a lengthy review and approval process. However, domestic security intelligence products do not endure the same scrutiny since they are not meant for widespread publication outside of security personnel. Any intelligence provided to security programs often includes relevant threat information used to determine risk levels for internal decision makers who must act based on that information. In the event an intelligence product would add value to the IC, the analysts coordinate with the customer's intelligence directorate to comply with their publication process and release authority. However, most intelligence used by security personnel is derived from finished intelligence already published by the intelligence community, most specifically the DoJ and DHS given restrictions on DoD's ability to collect on US persons.

## 1.1 National Intelligence Disciplines

The National Geospatial Intelligence Agency (NGA) leads the DoD's efforts in Geospatial Intelligence (GEOINT), which can be characterized as the IC's eyes. This discipline involves sophisticated imagery collection assets that captures photos and videos on areas of interest. The collection platforms include Unmanned Aerial Systems and satellites that are built, flown, and maintained by the National Reconnaissance Office.[10] The NGA's contributions to the Global War on Terror led to an exact replica of Osama bin Laden's compound for SEAL Team 6's rehearsals before the raid and has also correctly predicted where insurgents may have conducted IED strikes in Iraq.[11] GEOINT could be applied to security programs by planning the best egress/ingress routes for first responders, or determining the most likely avenues of approach for aggressors.

[10] National Reconnaissance Office. About The NRO. (N.d.)

[11] Brown, D. 10 Things You Might Not Know about the National Geospatial-Intelligence Agency. (2013, March 22).

The National Security Agency is the leader in Signal Intelligence (SIGINT), and serves as the IC's ears. Like most Combat Support Agencies, the NSA's existence was classified for a long time before becoming public knowledge. The acronym 'NSA' was satirically referred to as meaning 'No Such Agency' instead of its actual meaning because of how seriously its employees took operational security. However, all their efforts pertain to some form of an electronic signal and can involve communications systems, weapons, and radars used by adversaries. The NSA is tasked with eavesdropping and making/breaking codes in order to defeat the U.S.' national security threats.[12] They are also the leader in the defense of the cyber domain, where they protect the U.S.' cyber assets. Their application to a security program could come from intercepting a message about a pending attack on a government agency or CDC. Knowing about a potential attack beforehand would enable the agency to better prepare or thwart it.

The Central Intelligence Agency is an independent organization and their official mission is to "collect, analyze, evaluate, and disseminate foreign intelligence to assist the President and senior US government policymakers in making decisions relating to national security".[13] While it is likely they use multiple disciplines of intelligence, the CIA is widely known to be the premier Human Intelligence (HUMINT) agency. They are capable of clandestinely acquiring photographs, documents and conducting overt collection overseas. They also maintain official contacts with foreign governments and debrief foreign nationals in addition to U.S. citizens who travel overseas.[14] Regardless of how they fuse intelligence disciplines, their ability to interact with people for the collection of intelligence is what makes them different from the aforementioned agencies and disciplines. Since it is not within the CIA's jurisdiction to collect on

[12] National Security Agency. What We Do. (N.d.)
[13] Central Intelligence Agency. About CIA. (N.d.)
[14] Ibid.

U.S. citizens, they may intercept and pass information to the Federal Bureau of Investigations (FBI) or DHS regarding a potential terror attack on a federal agency.

The Department of Justice's FBI is the U.S.' premier law enforcement agency that does have the jurisdiction to collect on U.S. citizens for the sake of investigations. The FBI is unlike the previously mentioned agencies as they do not specialize in a specific intelligence discipline and are primarily focused on federal investigations. The FBI has primary investigative responsibility on anything with a nexus to terrorism and weapons of mass destruction (WMD). This is significant because any local police department or another agency may discover leads that must be turned over to the FBI for investigation. Their investigations revolve around terrorism, counterintelligence, cybercrime, public corruption, civil rights, organized crime, white collar crime, violent crime, and WMDs. The FBI is known to be very good at counterintelligence, which is extremely crucial in security and a critical intelligence discipline in the security.

## 1.2 Security Intelligence

National intelligence focuses on illuminating threats for national security decisions, but for security purposes, security intelligence defines the operational environment and provides accurate threat data, driving a robust risk management cycle that enables security resources to be allocated according to an appropriate security posture. Consistent with the concentric circles of security, current intelligence will be analyzed from the outside-in to detect threats. A security programs intelligence personnel are be divided by two distinct focuses, all source intelligence and counterintelligence (CI). The all-source analysts will fuse finished intelligence reporting between the various disciplines to provide a single analytically sound intelligence estimate. The counterintelligence personnel will vary based on the type of customer; if they are a federal agency, they are badged and credentialed CI Special Agents, falling under that agency's federal authority. If the customer is a defense contractor, they may contract CI Special Agents or utilize CI analysts to conduct similar analysis as their federal counterparts. The CDCs also maintain near constant coordination with CI Special Agents to ensure compliance with their sensitive programs and all security countermeasures are being followed.

Unlike for national security, a security program's intelligence collection assets are limited to technical tools that collect and analyze network data in a security operations center.  Without nonorganic or multispectral collection assets, all-source analysts may still reap the benefits of those tools through integration with the IC, in order to receive finished intelligence (FININT) reports that may illuminate a relevant threat to the customer. Integration into the IC facilitates information superiority that may prevent an attack and is imperative in providing accurate data used for risk analysis. This responsibility may be accomplished through networking and personal relationships with other agencies. It is also made possible by the intelligence personnel working with Intelligence Directorates and maintaining their Top-Secret clearances with the additionally required caveats. Maintaining strong relationships in the IC also enables security personnel to submit requests for information (RFI) with a higher likelihood of having them answered by a subject matter expert.

Exemplifying the added value of submitting RFIs, the FBI posted one in March of 2019 regarding the integrated analytic capabilities across media channels. However, based on security clearances, risk analysts may not share the same level of access to intelligence reports. This implies a strong need for mutual trust between the intelligence and risk personnel when vague intelligence assessments are made for the sake of benefiting from risk analysis, just without all the details of the report. Like the tipping and queuing of information that should occur between departments, can occur internally between the intelligence analysts and the risk and security personnel.

Sharing information between federal, state, and local government entities along with industrial partners is so crucial that the Department of Homeland Security created 80 fusion centers across the U.S. for this purpose. Each center serves as a regional focal point where contributing members offer threat data that benefits and may protect others. The diversity among members' missions and proficiencies enables increased situational awareness for everyone and provides a level of interdisciplinary expertise they would not be able to achieve individually. Additionally, each center's intelligence products are shared through the Homeland Security Information Network (HSIN), making their findings easily disseminated to all the other Fusion Centers and their members.

The information analyzed and shared with the Fusion Centers depends on the threat landscape and may include cyber threat actors, indicators of compromise (IP Addresses), criminal threats like fraud, and any terror related activity. Ensuring security intelligence analysts are active members in their nearest Fusion Center is imperative to accomplishing their responsibilities. Individual security programs contribute to the Fusion Centers, but official products are approved by the senior intelligence analyst within the customer's intelligence directorate. The exception to this requirement is updates on real time events or attacks, such as malicious IP addresses or a threat changing locations.

Effective security programs differ from traditional ones because they are not built in silos, thus enabling them to handle any situation with internal capabilities and proficiencies. Many security programs are comprised of multiple departments, making the requisite coordination to accomplish protection objectives difficult. An example of how integrating intelligence accomplishes true security fusion is how they share information with the IT department / Security Operations Center (SOC). Depending on the size of the organization, at least one analyst will be assigned to the SOC, along with physical and information security personnel. In many organizations, the SOC is solely managed by the IT department; however, intelligence analysts have a significant stake in the organization's SOC as they should be aware of what attacks are being defended against for attribution purposes. Intelligence personnel playing an active role in the SOC enables security intelligence to communicate hasty indicators, or alerts that may change the threat landscape, ultimately elevating the security posture in real time. Additionally, any information processed between the SOC and the analysts will add value to the Fusion Centers when shared.

The all-source intelligence analyst's main objectives are to evaluate ongoing threats and analyze the external operational environment (OE). While collection and analysis on both must remain a constant effort, analyzing the OE is initiated more generally in order to first identify the threats, which counterintelligence efforts focus on in more detail. However, it is imperative to understand the contrast between the security programs OE and the agency's potential OE. If the customer's facility is hypothetically located in Baltimore, Maryland, the customer's OE is the city and surrounding areas within proximity. While the agency is physically in Baltimore, their mission set may focus on a country, or countries, in the Middle East where assets are deployed, making that their OE, not the city they are located. Per the DoD's Joint Publication 2-01.3, 2014, "the operational environment is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander." For holistic security, the decisions will determine the allocation of security resources and influence the customer's security posture. The OE can be further described as the totality of operational variables within proximity of the customer. The variables may include infrastructure, social mores, politics, key personnel, and the way they all fuse together at any given time.  All these elements are determined and analyzed by intelligence analysts.

A key element of the Joint Publication's definition is 'influence' because it may be an indicator of threat probability. If the OE favors the customer's presence, the likelihood of vandalism and other crimes decreases. However, if the location's population negatively views the customer, they may be easily influenced to attack the facility or employees, even outside of the facility. This threat occurred in 1993 when a Pakistani man shot and killed two CIA employees on their way to work at the CIA headquarters in Langley, Virginia. The attacker claimed his motivation was anger about U.S. policy in the Middle East, which indicates he believed the CIA's actions went against his beliefs.[15] The most crucial point of this tragedy, in regards to the security program, is how the customer's actions outside of the OE can influence behavior within the security program's OE. Intelligence analysts will not have a need to know details about what operations the customer may be conducting, but a general understanding of the affected regions will provide insight about potential threats in the program's OE and the intelligence personnel will be privy to that information through their relationships with the customer's intelligence directorate. Additionally, their collection efforts of regional atmospherics will provide useful intelligence used to determine the programs overall security posture.

Analyzing the OE must remain a cyclical effort as it is likely to develop rapidly. It is imperative for the intelligence analysts to always continue collecting on the cyber and information domains in addition to physical atmospherics as they all contribute to shaping the

[15] Central Intelligence Agency. Killer of CIA Officers at HQs Convicted (2017.)

OE. The main OE questions that will provide the most actionable intelligence for the program's other facets are as follows:

- What is the surrounding population's general attitude/public opinion towards the customer? The public's attitude towards the organization impacts security in many ways because it influences every interaction and the employees' safety. Additionally, the customer's employees are drawn from the local talent pool, which may affect the quantity and quality of those interested in working there. The resolve of employees may also indicate a heightened counterintelligence threat.[16]
- Are there major events occurring that impact operations? This is important because large events may cause a change in response times and change the population make up.
- Who/what are the key influencers (people, places, organizations) that draw the most public attention? Defining the societal pillars of influence enable intelligence personnel to constantly monitor and estimate the proverbial pulse of society. This element will likely include political personnel and parties.
- Who could benefit from attacking the customer? This could include an organization, a person, or a nation. It is important because it will direct intelligence collection efforts and allow the intelligence personnel to further analyze the threats.
- Are there signs of whomever may benefit from attacking the customer in the OE? This strictly refers to physical presence because cyber threat actors will always be

[16] Center for Development Security Excellence. Insider Threat Awareness, INT 101 Guide. (N.d.)

present in the cyber domain. However, monitoring potential attacker's activity when physically present, or their presence alone if it is unusual, may indicate a need for heightened security.

- Are nefarious IP addresses accessing the customer's network? Third party companies, such as Recorded Future, provide a security service where they share IP Address Intelligence Cards. The IP Address Cards serve as a summary of essential information pertaining to an IP address and an associated risk score.[17] Understanding which IP addresses are associated with malicious behavior allows the customer to prevent their access to their network and reduce the potential for an attack. This level of current information gathering requires collaboration with industry partners, and the IC as the same blacklisted IP addresses commonly target more than one victim. This is how the IP addresses become known and blacklisted, but that only helps if the information is shared and reviewed by professionals. The malicious IP addresses are normally shared through the Fusion Centers, which further exemplifies the security program's need to be connected to HSIN.
- What cultural considerations are expected as normal social behavior? Understanding cultural norms enables the security program to better provide the 'customer service' aspect of security by ensuring interpersonal and communication practices compliance; in effort to prevent or de-escalate any situation that could entice or create a threat. Additionally, knowing the normal

[17] Recorded Future. IP Address Cards. (N.d.)

social behavior and training security personnel on it will enable them to realize the absence of normal or unusual behavior that may indicate a threat.

Maintaining a current understanding of the OE ensures analysts will consequently understand the threat actors within it. By accurately recognizing and perceiving the threats, security can produce a far more accurate risk assessment than a risk management cycle that does not place much emphasis on analyzing OE information. However, collecting and estimating threat actor details is substantially more difficult due to the cyber domain. The intelligence analysts' efforts monitoring data in the SOC will be crucial to accomplishing this objective. As attacks occur, cyber threat analysts will investigate their origins and assign attribution characteristics. This information is documented in a security information and event management system (SIEM), which will help identify patterns and provide vulnerability alerts. Non-attack information, such as data flows, telemetry, packet captures, syslog (message logging), and user account behavior will also be collected and analyzed to identify potential indicators of compromise.[18] Of note, the FBI created Threat Assessment Teams who specialize in this type of analysis.

## 1.3 Counterintelligence

The risk of spies in the Intelligence Community is more prolific than ever before, which makes counterintelligence a crucial element of security intelligence operations. The Dictionary of Military and Associated Terms, 2005, defines counterintelligence as "activities concerned with identifying and counteracting the threat to security posed by hostile intelligence organizations or by individuals engaged in espionage or sabotage or subversion or terrorism."  The term 'Foreign intelligence entities' (FIE) is now most used in place of hostile intelligence organizations.

[18] Exabeam, Log Aggregation, Processing and Analysis for Security. (N.d)

However, their threat remains high as the FIEs recruit and emplace people like Ana Montes, Aldrich Ames, and Robert Hanssen to steal U.S. secrets and spot potential spies. CI Agents work cooperatively with their cyber counterparts to investigate matters associated with the national security crimes outlined in AR 381-12. Their efforts will be derived from the customer's Insider Threat program, which security programs are responsible for managing, and plays an integral role in the task of security intelligence and countering FIEs.

Of all the threats facing the Intelligence Community, the threat of insiders stealing and leaking sensitive data remains the greatest security challenge to customers working in national security. Unfortunately, the digital world and global connectivity fosters an environment for insiders to quickly transfer large amounts of protected information to outsiders with a reduced likelihood of detection, as evidenced with perpetrators like Snowden. Plus, cyber countermeasures make remote hacking a very difficult task, making physical vulnerabilities the easiest to exploit from the inside. There are myriad reasons why insiders conduct espionage or steal information, but the damage to the security program's customers can have fatal consequences, regardless of what the motivation is. Therefore, it is imperative for CI Agents to detect, deny, and defend against their efforts before the damage is done.

The National Cybersecurity and Communications Integration Center defines Insider Threat as "a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems. Insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices."[19] Again, this definition closely aligns with the others who conduct intelligence for the security objectives. Insiders conduct attacks in every industry, but attacks within the intelligence community can cause far more serious consequences than those in private industry where only money is lost. When classified intelligence is leaked, it can provide nation-state competitors, or nefarious criminal enterprises, a strategic advantage by knowing what the U.S.' actual objectives or motivations may be. Leaked intelligence can also provide a tactical advantage to adversaries if they use the information to conduct offensive counterintelligence operations against the security program's customers. An example of this would be with Aldrich Ames in his attacks.

Insiders may attack in many forms or, in some cases, not even know the damage they are causing. When classified information is leaked unintentionally, despite best efforts to safeguard it, the actors are known as careless or naïve insiders. The CERT Insider Threat team, part of Carnegie Mellon University's Software Engineering Institute, coined the term – unintentional insider threat (UIT). Their term, UIT, accounts for incidents when the protected information is accidentally disclosed on a website, mishandled in an unsecure environment, or inadvertently sent to the wrong party via email, fax, or mail.[20] It also accounts for when users are hacked either through social engineering, phishing attempts, or malware/spyware. Lastly, UIT includes breaches where an insider mistakenly carries an unauthorized mobile device into a SCIF or secure area that can be compromised, or misplaces/incorrectly discards data.[21] It is likely that insiders do not self-report when they conduct some of these actions, making accurate data loss

[19] National Cybersecurity and Communications Integration Center, Combating the Insider Threat. (2014)
[20] Software Engineering Institute, Unintentional Insider Threats: A foundational Study. (2013).
[21] Ibid.

impossible to calculate. These are all examples of situations CI Agents would investigate, but security is tasked with mitigation and prevention.

The greatest challenge CI Agents face with identifying malicious insiders is the fact that they are authorized users, usually conducting authorized matters of business, but with ulterior motivations. Their authorized activity makes it extremely difficult to measure their intent without creating false suspicion of an innocent employee, or alerting an actual insider that they are caught. This challenge is exacerbated by the fact that system administrators have little chance of recognizing when an employee is doing something malicious if they stay within the scope of their job. Operators in the SOC use User Activity Monitoring (UAM) tools to analyze a user's activity on the customer's network. The UAMs monitor the user's endpoints and establishes patterns of behavior for how they interact with files and folders. A similar tool, also used by SOC operators, is User Behavior Analytics (UBA). The UBA also analyzes user behavior, but with the sole purpose of detecting threat. Through machine learning, the UBA is effective at detecting outliers, or anomalies, that may be indicative of a threat. The UBA differs from the UAM because it focuses on data collected from networks, hosts, and cloud environments, not just endpoints as the UAM relies on. Another tool used to determine indicators of compromise is Data Loss Prevention (DLP). Meant to catch data-use policy violations and leakage, DLPs provide the analysts another valuable tool.[22] However, they require extensive data discovery and manpower to be effective and this is where working side-by-side with IT's network analysts is imperative. Once the indicators of compromise are discovered, that evidence is passed to the CI Agents for further investigation.

[22] ObserveIT, Do You Know Which Cybersecurity Tools Really Address Insider Threat?. (2018)

Another area of CI focus that is crucial to security is that of background investigations for security clearances since the customer's employees are all likely to possess one. Clearances are based on the hiring official's determination of each position's duties and responsibilities. The purpose of a security clearance is to determine whether an individual is trustworthy and competent enough to safeguard classified information. The background investigations required for clearances vary depending on the level required, but may include polygraphs and take years to conclude. Throughout the background investigations, many facets of the subject's life will be analyzed to determine their loyalty, character, and reliability. Additionally, periodic reinvestigations are required every six years to ensure no negative changes have occurred in the subject's character or ability to safeguard classified information.

In September 2019, a significant change to the background investigation and the security clearance process occurred with President Trump signing Executive Order 13869. Prior to the new EO, the Office of Personnel Management (OPM) had the primary responsibly of conducting the investigations. However, EO 13869 mandated the Defense Counterintelligence and Security Agency will realign with a newly created organization called the National Background Investigations Bureau and maintain primacy for the clearance and investigation process.[23,24] OPM was fraught with issues, making this executive action a significant effort in improving security and counterintelligence efforts.

## 1.4 Insider Threat Program

All the data collected and processed between security clearance investigations and in the SOC serve as only a portion of the insider threat program. Per Executive Order 13587, federal

[23] National Background Investigations Bureau. NBIB News. (2019)

[24] White House. National Security and Defense. (2019)

organizations will conduct insider threat response actions and comply with all the outlined general responsibilities and requirements, while simultaneously improving the efficiency of the program and serving as the central program office. Assuming the role of the central program office, as delineated by the Director of National Intelligence's National Insider Threat Task Force guide (NITTF), enables security to initiate action and responses more quickly by removing bureaucracy and the need to include other departments until necessary.[25] Insider threat programs provide the status of maturity framework elements and incident reports to senior leadership on a monthly basis. To answer the dynamic requirements of the insider threat problem set, insider threat programs use the NITTF's maturity framework to enhance the minimum standards. Regardless of who the customer is, insider threat programs will incorporate the following elements, which were derived from Executive Order 15587 and best practices outlined by the FBI, Defense Security Service, and the National Counterintelligence and Security Center to reduce risk:

- Know the customer's critical assets. Understanding what the customer's assets are enables security to build countermeasures that effectively protect against them. It also helps identify who may be a threat by understanding what value the assets are. For federal agencies, assets may include networks, intelligence collection systems, people, classified information, or sensitive personnel data.
- Document and enforce policies and controls. To influence compliance with effective security practices, expectations need to be well documented and disseminated to all those who are expected to obey them. Documenting incidents

[25] National Insider Threat Task Force, NITTF Mission. (N.d.)

and creating policies also educates people and builds situational awareness for the customers.

- Analyze threats to assets. First the threats must be identified, either physical or cyber. Once identified, they must be profiled and cataloged for analysts to use as information develops, which may lead to patterns. The analysis must also be shared through fusion centers and with IC partners to either learn more or provide situational awareness to others. It is imperative to understand what the threat wants to attack, what motivates them, how they operate and what specific vulnerabilities they have the capabilities of exploiting.
- Determining vulnerabilities. After knowing what the customer's assets are, risk assessments identify and quantify vulnerabilities. This involves first identifying key assets and analyzing their value, placement, and the countermeasures guarding them. The vulnerabilities could include poorly trained personnel, malfunctioning security equipment, or a poor physical placement of the asset. For budget constraints, vulnerabilities are to be mitigated based on the criticality of the asset, its impact if lost, and likelihood of the associated threat, as defined by intelligence driven risk management.
- Conduct in depth risk assessments. The risk management personnel's assessments will provide the customer's overall risk rating by quantifying the threats, their likelihood of attack, the customer's vulnerabilities, and estimating the impact of a breach or loss of an asset. Most of the data used by risk analysts is provided by intelligence analysis. The risk assessments are updated constantly, reflecting the ever-evolving OE and threat landscape. As risk ratings increase or decrease, the

security posture will adapt accordingly. Examples of risk are not always as glaring as terrorism or espionage and can include insufficient training, alcohol use, or even a lack of policies.

- Implement countermeasures to address the threats and reduce risk that comply with minimum standards set by the National Counterintelligence and Security Center and NITTF. Based on the risk rating, security practices and countermeasures will be implemented to mitigate the associated risk. An elevated risk rating infers a more imminent possibility of attack. As the risk rating increases, a more aggressive security posture will mean stricter policies and less liberties until the threat is reduced. It may also mean travel is revoked or limited, large events are postponed, and passwords will need to be changed more frequently.
- Monitor and respond to indicators of compromise. The designed and implemented countermeasures will include procedures for responding to attacks. The SOC will prepare for threats based on shared intelligence and manage all cyber incidents. Physical incidents are managed by emergency response personnel in accordance with the policies and regulations in place.
- Conduct continuous review and training for employees and security personnel. It is imperative that a lifecycle management plan be incorporated into every process. Equally important is training the customer's employees as a lack of situational awareness or understanding how to respond to certain situations may enable the attacker to remain undetected. Through training, employees will know how to report suspicious behavior and learn about recent events. Training for employees

is best conducted once per year and mandatory online refresher training helps augment in between.

- Consider the workplace environment. Fostering a positive and productive workplace reduces stress-caused disillusionment that may influence an employee to become a threat. Plus, the happier a workforce is, the more productive they are. In national security jobs, the stress may be higher than other careers where health and safety are not at risk. Encouraging innovation, rewarding performance, and cutting meeting times are free and simple things a customer may implement to improve moral and employee engagement.[26]

Another dynamic aspect of the CI Agents' responsibilities is 'red teaming' the customer's facilities and security's countermeasures. The term 'red teaming' has many definitions, but federal programs adhere to the DoD's FM 34-60, 1995, description, which is hostile intelligence simulation. To better identify and assess vulnerabilities that are reported to risk analysts, red team operations occur as requested by leaders or as threat specific tactics, techniques, and procedures are learned. CI personnel coordinate and execute a simulated FIE attack against specified targets of interest as realistically as possible. Social engineering is a significant part of red teaming, so other department's employees may be recruited to conduct attacks for the exercise since most employees are likely cognizant of the personnel's identity and true intentions. The red team's objectives may include breaching physical countermeasures or illicitly accessing the customer's network.

## Chapter 1: Conclusion

[26] SHRM Foundation, Employee Engagement and Commitment. (2006)

Integrating intelligence operations into security programs is essential for federal organizations tasked with national security objectives. For any security program to be commensurate of its associated risk, constant analysis is required to ensure current information is being used for decision making. The process of collecting and analyzing that information is how intelligence operations supports security programs; it makes them more cost efficient, more proactive, and enables them to offer a more deliberate service to their customer.

Intelligence drives the risk management and security operations cycles through ongoing threat and vulnerability assessments. As changes occur within the threat landscape, the program's posture can adjust accordingly. In many cases, this involves allocating additional resources or implementing threat-specific countermeasures. Without ongoing intelligence, security programs are either based on a guess or old data. Additionally, intelligence is used to adequately assess the operational environment, which is how analysts know where to begin looking for threat data.

Security programs that make intelligence an integral aspect of their program also enjoy increased collaboration within their organization. Many federal mandates require such teamwork, but programs benefit the most when it is organic as it decreases the potential seams in the customer's overall protection; seams that attackers are known to exploit. Additionally, intelligence enables the security program to offer valuable information to regional fusion centers, therefore, there is potential they may make an impact on another organization's protection as well. Examples of internal coordination are between physical, information (cyber), and personnel security departments, and even with other business departments such as IT, Human Resources, and supply chain management.

There are many disciplines of intelligence that could all be used for security intelligence, but the two most common are open source intelligence and counterintelligence. Open source is used to gather crucial information in risk research, atmospherics, and analyzing the customer's digital footprint. Counterintelligence is vital for insider threat programs, which is a significant threat in today's environment. Counterintelligence is also used to conduct investigations and counter attacks by foreign intelligence entities. When used effectively, intelligence undoubtedly improves security. Unfortunately, the involvement of intelligence in security does not often get the credit it deserves due to the nature of its success equating to prevented and subsequently unknown attacks. The relationship between intelligence and security only received publicity after events from attackers such as Ana Montes, Edward Snowden, Nidal Hassan.

Intelligence is the lifeblood of any holistic security program. Not only does it drive the risk management practices that influences countermeasures, it also impacts ancillary facets of the organization such as emergency response and crisis management. Additionally, intelligence is a timeless asset that extends beyond the role and responsibility of security; it effects supply chain management, public affairs, and human resources – creating an environment that benefits from applying a holistic security template.

## Chapter 2: Risk Management in Security

Security programs exist to protect people, places, and information from traditional and emergent risks. Security is necessary because it reduces the impact of isolated, non-malicious incidents along with the more serious events like cyberespionage and workplace violence. In serving its role, security programs are customer focused and provide both reactive and proactive countermeasures that achieve the organization's desired protection. A risk-based approach to security involves balancing between funding constraints and requisite levels of security, based on proactive analysis of each facility's risks.[27] This process stewards effective security risk management practices, which increases the organization's level of protection. However, stubborn workplace cultures and limited threat information create challenges to using security risk management most effectively.

It is difficult for federal security programs to adapt to their ever-changing threat landscapes and the risk is amplified by the likelihood a security event will echo far outside the compromised organization, potentially impacting national security. The threat landscape is more complex and advanced than what many other industries face due to the nature and capability of the U.S. government's adversaries, especially given the advancements in technology and growing prevalence of cyberwarfare. However, federal security programs that effectively use risk management principles to augment their security strategy are more likely to protect their organizations successfully. The objective of this chapter is to illuminate what role risk management plays in federal security programs and articulate how it increases protection. By analyzing previous risk events, the determination was made that analyzing risk factors and consequently applying the principles of risk management can improve efficiency of federal security programs. The 2013 security breach perpetrated by Edward Snowden had a profound impact on moving the DoD toward a more risk informed culture, making it more difficult for future attackers to have the same effect.

There are innumerable risk events throughout federal workplaces. However, many do not directly pertain to security, like reputation damage, poor organizational financial decisions, or pandemics such as COVID19. To better describe how risk management works symbiotically

[27] Congressional Hearing, 113 Congress. Facility Protection: Implications of the Navy Yard Shooting. (2013)

with security programs, this thesis installment will use real-world cases for both cyber and physical events that exemplify specific points. Applying risk methodologies in consideration of similar events will increase the likelihood of preventing them, better prepare the victim to respond, and further reduce the impact since security events are inevitable. The federal workplaces include any place of employment where federal employees go to work on achieving national security objectives within the continental US. They may include federal intelligence agency headquarters buildings, military bases, or annex buildings of any federal organization.

There are a plethora of regulatory requirements and risk frameworks available to the federal customers, yet most risk management decisions have the potential to be made only at the senior leadership level and not given much consideration by middle management down to the actual security personnel. The Armed Forces, of the Department of Defense (DOD), use a Force Protection Condition (FPCON) model, which the Geographic Combatant Commanders use to dictate the security postures of their facilities.[28] When an FPCON is assigned, a canned set of security measures are followed based on a policy written to address a generic risk level. This is problematic because the threats that influence risk are dynamic and do not neatly fit into generic classifications, creating institutional vulnerability. Perhaps this is a weakness of the culture where employees are expected to simply follow orders without offering any sort of critical thinking, or maybe there are not enough details communicated about the change in threat information.

Regardless, the practice of blindly allocating security resources without calculated rationale based on risk factors is merely guesswork, not effective security planning and the

[28] Department of Defense Instructions, DoDI O-2000.16 Volume 1. (2017)

reason applying risk management to daily security activities is necessary for improved protection. As this thesis will demonstrate, the Department of Homeland Security (DHS) is the federal leader at integrating risk in every business decision for the sake of national security, creating an example for the DOD to follow. However, it is likely that other federal organizations, such as the Bureau of the Census and the Internal Revenue System (IRS), have stronger risk cultures than the DHS; the difference being the IRS and Census Bureau are not utilizing risk management practices to improve national security. 1

An issue with security in every industry is the fact that it is always an overhead expense and never the purpose or strategic objective of the organization it serves. The same is true with federal organizations whose strategic objectives are national security related, not day to day security of a facility. The organizations often execute intelligence driven operations, investigations, and missions that support the requisite activities associated with protecting the homeland and interests abroad. Their activities may include developing new defense technology or assets, training defense personnel, investigating terror plots, or executing national security operations. Regardless, security operations are ancillary to many organizations' main efforts. Security departments are essential to a safe working environment, but can be compared to other support elements like logistics, legal counsel, human resources, and maintenance in the eyes of senior leadership.

Within the realm of security, there are many distinct disciplines: physical, information (includes cyber), operational, and personnel. The distinction is important because each discipline is usually its own department, or branch, and managed by different leaders within each organization. This leads to each security department being treated as a different system, which creates silos and unilateral decision making, despite how they depend on one another.[29] In 2018, federal agencies submitted 31,107 cyber-attack incident reports, which warrants a higher amount of attention given to cybersecurity and proves they are constantly under attack.[30] This operational silo approach causes differing risk practices, a lack of coordination/communication between the analogous teams, and departmental seams that present vulnerabilities, which are increasingly exploited by adversaries.[31] However, cybersecurity departments differ from their physical-security counterparts in their usage of security risk management; the objectives differ between defending against a virtual network and a physical facility.

There seems to be a very present and concerted effort to practice sound risk management within cybersecurity, but bureaucracy, the complexity of the virtual domain, and ever-evolving threats make it more of a challenge than physical. In 2018, Homeland Security Secretary, Kirstjen Nielsen, reported to a Senate Homeland Security committee that "cyberspace is the most active battlefield," and her top priority.[32] As a result, Secretary Nielsen created the Cybersecurity and Infrastructure Agency (CISA) as an element of the DHS in response to her concerns about cybersecurity. CISA improves the protection of the nation's critical infrastructure from both physical and cyber threats by improving communication and coordination. CISA provides comprehensive cyber protection, coordinates infrastructure resilience, emergency communications, and manages the National Risk Management Center.[33] Given the DHS's mission of protecting the homeland, they have historically championed facility security practices. However, lessons learned from previous risk events caused their efforts to include incorporating

[29] John Carney. Cisco, Why Integrate Physical and Logical Security. (2011)
[30] J. Clement. Statista, Annual Number of Cyber Incidents. (2020)
[31] Mike Burmester. Florida State University, Modeling Security in Cyber-Physical Systems. (N.d.)
[32] Breanne Deppisch. Politico, DHS Was Finally Getting Serious About Cybersecurity. Then Came Trump. (2019)
[33] Cybersecurity & Infrastructure Security Agency. (N.d.)

risk management for the sake of improving security's proactiveness and increasing its chances of preventing an event and/or reducing its impact.

As this thesis installment will demonstrate, there is a strong nexus between risk management and security programs, making the customers far more secure. The paper will begin by providing a history on risk management within the government, because of the significant events that influenced where it stands today. Following the history, the importance of risk-communication and clearly defining risk terms will be discussed, setting the stage for the risk model. The risk model section will go through each step and use event-based examples to articulate the importance of each.

## History of Risk Management in Government

The value of applying risk methodology throughout the government became apparent in 2016 when Circular No. A-123 was updated, mandating all federal agencies apply enterprise risk management (ERM) in pursuit of their strategic objectives.[34] Circular No. A-123 was significant because it created the requirement  for organizations to use ERM as an internal control when they may not have previously done so. The act was managed by the administration's Office of Management and Budget (OMB) and placed significant emphasis on involving management in the process. Additionally, it created an avenue of accountability for financial responsibilities as it was published under the Federal Managers' Financial Integrity Act (FMFIA).[35] The implementation of the circular was a step closer to having ERM applied to security programs, but its emphasis on financial decision making and its intended application on "strategic objectives"

[34] Michael Keegan. Government Executive, How Risk is Transforming Government. (2017)
[35] Shaun Donovan. Executive Office of the President, OMB Circular No. A-123. (2016)

makes it an unlikely consideration of security practitioners in their day to day security operations.

In 1995, President Bill Clinton issued Executive Order 12977, which coordinated security initiatives throughout the government and created the Interagency Security Committee (ISC).[36] The establishment of the ISC was the President's response to the bombing of the Alfred P. Murrah Federal Building, in Oklahoma City, which killed 168 people in the federal facility and injured nearly 700 others.[37] On 17 April 2020, the current ISC Chairman, Mr. Brian M. Harrell, released a letter to federal facility security stakeholders that stated, "The aftermath of the bombing of the Murrah Building led to sweeping changes in how the U.S. Government approaches preventive security and protection of federal infrastructure."[38] Mr. Harrell was partially speaking to how risk management became part of ensuring security was preventative instead of reactive, as it was prior to the attack. The ISC was initially led by the General Services Administration (GSA), until the creation of the Department of Homeland Security (DHS), which now chairs it and tasked CISA with its oversight.[39,40] 40 United States Code (U.S.C.) § 1315, the Presidential Policy Directive (PPD-21), and the National Infrastructure Protection Plan (NIPP) are foundational documents that codify DHS's responsibility for protecting buildings, grounds, and property that are owned, occupied, or secured by the Federal Government; establish U.S. policy for enhancing protection and resilience of the Nation's critical infrastructure; and provide a framework for integrating efforts designed to enhance the safety of critical infrastructure.[41]

[36] The American Presidency Project. Executive Order 12977 – Interagency Security Committee. (1995)
[37] Clinical Orthopedics and Related Research. Mass Causalities in the Oklahoma City Bombing. (2004)
[38] Brian Harrell. Interagency Security Committee. (2020)
[39] Shawn Reese. Congressional Research Service. Federal Building and Facility Security. (2017)
[40] Cybersecurity Infrastructure and Security Agency, Interagency Security Committee. (N.d.)
[41] Interagency Security Committee. The Risk Management Process for Federal Facilities. (2016)

Through its creation of policies and assistance with implementation of standardized security risk processes, the ISC has been instrumental in establishing a strong federal security strategy in response to the aforementioned federal guidelines and requirements. The ISC's efforts consist of regular working groups of security subject matter experts from 64 federal agencies, making the collaboration of prevention focused security standards more achievable.[42] In addition to ISC's collaborative efforts, the executive order encouraged organizations to share security related intelligence with other federal organizations in a timely manner, which empowers organizations to update their risk levels and security practices based on current information.

The sharing of critical threat information reduces risk by enabling security programs to potentially make better, more informed operational decisions instead of working without a complete understanding of the operational environment. The Ft. Hood shooting, in 2009, is an unfortunate example of how sharing information on attack indicators could save lives. Both the FBI and DOD had important information on the shooter, but their failure to communicate the threat data resulted in each department missing information the other had and not acting.[43] Consequently, 13 lives were lost by not communicating and understanding the actual risk the shooter presented.

To physically carry out and standardize security, the Federal Protective Service (FPS) was established as part of the Department of Homeland Security (DHS). The FPS is responsible for ensuring safe and secure workplaces at approximately 9,500 federal facilities.[44] The FPS takes the lead on ensuring building security by publishing emergency event plans, conducting assessments, and providing guidance on building new facilities. Additionally, the FPS has

[42] Brian Harrell. Interagency Security Committee. (2020)
[43] Congressional Hearing. House Hearing, 112 Congress, Lessons from Fort Hood. (2012)
[44] Department of Homeland Security. The Federal Protective Service. (N.d.)

operational law enforcement officers who respond to threats with their specialty teams, such as Explosive Canine Detection and Hazardous Response. However, the creation of ISC dramatically shifted FPS's mission from building-security to one of law enforcement and threat mitigation.[45] They accomplish their mission by identifying and mitigating security vulnerabilities through ensuring qualified individuals are on guard and using technology and collaboration as a force multiplier in their operations. ISC and FPS account for a significant amount of the government's ability to implement risk management into security as their efforts are what make it possible.

In 2016, the ISC published an interagency standard for risk management at federal facilities, likely in response to the circular. To assist with the implementation of the circular, the OMB also created an enterprise risk management (ERM) playbook that can be used in conjunction with the ISC's risk management standard. OMB's playbook provides key concepts and guidance for agency management to update their internal controls and modernize their risk management efforts.[46] It was created by risk practitioners and cross functional representatives from over 20 agencies to ensure it met the requirements of each organization. Between these resources and the support offered by the FPS, federal organizations have an abundance of security risk management guidance and publications to use in their risk management efforts.

## Defining Risk Management and Federal Facility Security

There are many terms used to discuss planning for and understanding undesired events within an organization. The DHS's Risk Lexicon defines risk management as "a process of

[45] Brian Harrell. Interagency Security Committee. (2020)

[46] U.S. General Services Administration. GSA Launches Enterprise Risk Management Playbook. (2016)

identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken."[47] However, risk management is often departmentalized and fails to account for implications outside of a given department. It combines threat information, internal vulnerabilities, and the estimated impact of a potential event to create a quantifiable risk level or score. Alternatively, ERM is used as an extension of traditional risk management and considers the risk level to the entire organization, but the success imperative is communicating risk information throughout the organization. Consistent with the guidance put out by the executive office's circular, ERM is strategic and requires more involvement from senior leaders to ensure risk is evaluated in a holistic fashion.[48] Both ERM and traditional risk management are meant to be ongoing processes that help organizations control and reduce their risk level through a more informed decision-making cycle.

At the onset of the circular, all agencies were mandated to generate an initial risk register, which provided details to senior leaders on the risks to their organization. This process enabled the senior leaders to determine their risk appetite, which is the amount of risk their organization is willing to accept in pursuit of its objectives.[49] The determination of an organization's risk appetite is communicated through a risk appetite statement, where the amount and type of risk the organization accepts is communicated and used to ensure each department or branch is operating within the bounds of its tolerance. Additionally, the risk appetite statement is instrumental at influencing the organization's attitude towards risk because it shows there is buy-in from senior leaders who approve it. However, the risk appetite is not optional; The

[47] Department of Homeland Security. Risk Management Fundamentals. (2011)

[48] Blackburn Group INC. Resources. (N.d.)

[49] Committee of Sponsoring Organization of the Treadway Commission. Understanding and Communicating Risk Management. (2012)

Government Performance and Results Act Modernization Act (GPRAMA) requires agencies to review and revise strategic plans every four years, which includes a review of their risk appetite and necessitates an analysis of the organization's holistic risk picture.[50]

As stated, the constant flow of information is what makes ERM successful. The two-way flow, between senior leaders and subordinates, enables security program managers to adapt their controls according to new strategies and, conversely, senior leaders can update their risk appetite based on emerging information. Additionally, this is how prioritization occurs, which allows security to focus on the fewer, but more significant, risks to improve the likelihood of mitigation. If risk priorities are not established and communicated, the security program stands to invest resources on many minor risks and not preventing the major ones as a result.

Federal facility security is implemented as a means of reducing an organization's risk. Its efforts include operations, personnel, and policies that reflect the unique needs of each organization. For security to appropriately allocate resources and plan, they must conduct thorough risk analysis through the assessment process. Security's operations may also include investigations, training, and emergency response. In 1995, the US Marshals Service created a rating scheme for classifying security levels of each facility:

Level I—buildings with no more than 2,500 square feet, 10 or fewer federal employees, and limited or no public access;

Level II—buildings with 2,500 to 80,000 square feet, 11 to 150 federal employees, and moderate public access;

[50] Chief Financial Officers Council. Enterprise Risk Management. (N.d.)

Level III—buildings with 80,000 to 150,000 square feet, 151 to 450 federal employees, and moderate to high public access;

Level IV—buildings with 150,000 square feet or more, more than 450 federal employees, and a high level of public access; and

Level V—buildings that are similar to Level IV but are considered critical to national security (e.g., the Pentagon).[51,52]

There are approximately 446,000 federal facilities across the US, ranging between every department and branch of the government. Of these, FPS monitors and provides security services at about 9,500, leaving other agencies to protect the rest.[53] To bolster FPS's coverage, they outsource protection to guard force management companies, equating to over 15,000 additional security officers standing guard at their facilities. Of the remaining 436,500 facilities, the manning of physical security is often left to the discretion of the various departments or agencies. According to the Department of Justice's Office of Justice Programs, there are over 20 federal law enforcement entities that protect many of the other facilities.[54]

## Communicating Risk Management

In 2016, the Government Accountability Office (GAO) conducted a study on how ERM has been implemented across the government. One of their key findings was the importance of an organization's senior leaders making risk management a part of the workplace culture. Without senior leadership's commitment to ERM, organizations are unlikely to take the extra

[51] Shawn Reese. Congressional Research Service. Federal Building and Facility Security. (2017)
[52] U.S. Department of Justice, U.S. Marshals Service, Vulnerability Assessment of Federal Facilities. (1995)
[53] Department of Homeland Security. Federal Protective Service Operations. (N.d.)
[54] Shawn Reese. Congressional Research Service. Federal Building and Facility Security. (2017)

time necessary to apply it in the decisions they make. Additionally, North Carolina State University discovered that if senior leaders fail to recognize the value of risk management, they become the greatest risk to the process. Their lack of support becomes a detriment to its potential success by increasing the chances that employees will ignore risk indicators or fail to communicate them effectively. Senior leaders can also impair the risk management process by ignoring risk factors themselves, working against the risk efforts for personal agendas, or by being nonexistent in the process.[55] Conversely, senior leaders can be the driving force at building a risk-informed culture through communicating its importance throughout the organization.

Communication, both internally and externally, is an essential aspect of making risk part of the workplace and protecting the organization; highlighting risks and finding pragmatic solutions can prevent catastrophes if it becomes the norm.[56] The GAO study reported one of the best practices they discovered was creating a "risk informed" culture where all employees can communicate risks according to the organizations reporting policy. Encouraging employees to raise risk concerns and openly discuss them fosters a positive workplace that promotes risk management and increases the chances of risk discovery.[57] This process is amplified if the organization's risk appetite is communicated throughout the ranks, making it known to the employees what senior leadership's priorities are.

Most federal security programs begin each shift with a roll call, which is shift change brief used to communicate current events or specific post orders to the oncoming shift.[58] The roll calls are effective opportunities to communicate risk considerations. If information was received

[55] NC State. Lack of Senior Manager Support Impairs Risk Management. (2012)
[56] Charles Clark. Government Executive, Agencies Get a New Playbook for Managing Risks. (2016)
[57] Government Accountability Office. GAO-17-63, Enterprise Risk Management. (2016)
[58] Robert S. Stering, Police Officer's Handbook: An Introductory Guide (N.d.)

that changed the threat landscape, security and/or law enforcement personnel would be able to adjust their procedures accordingly. However, communication must flow both ways between the security personnel and senior leaders. When information is discovered that changes the threat landscape, judgement must be made whether to report it to the senior leaders through the chain of command. Communicating security risks is an effective way to cause an organization's leadership to view those risks the same as other business risks, which also benefits security departments when funding decisions are being made.[59] Not every risk event is going to change the organization's risk level, but having middle management competent enough to critically consider the strategic implications of every event would make a significant impact on the relationship between senior leadership and middle management through added mutual trust. Additionally, training security personnel to consider risk to other departments, outside of security, is exactly what the circular and accompanying information on ERM intended.

Establishing information flow and communicating threat information laterally between departments is another crucial aspect for implementing risk management. Yet, the silos of physical security, personnel security, and information security create a lapse in that essential communication. The poor communication is likely a result of time constraints, or a false sense of reliance on the other departments to consider holistic implications. This breakdown of communication creates a significant vulnerability in the organization's protection when there is not a thorough awareness of the each other's strategy and challenges.[60] Many of the US government's adversaries use social engineering to enable their cyberattacks, accelerating the

[59] Rachelle Loyear. Risk and Resilience HUB, How Do You Communicate Security Risk to Business Executives?. (2019)

[60] Ileana Hamburg, Kira Grosh. Aligning a Cybersecurity Strategy with Communication Management in Organizations. (2018)

cyber and physical attack convergence.[61] It is challenging to connect dissimilar events, like a firewall breach and an unauthorized visitor wandering around the halls, especially when security personnel are usually understaffed and task saturated. However, communicating all suspicious events between departments may provide analysts the information they need to discover a new threat actively attacking the organization and give security the warning they need to prevent it.

A clear example of a recent blended physical-cyberattack was in March of 2020 when hackers from the FIN7 cyber-criminal group sent malicious USB drives disguised as Best Buy rewards to specific people at each targeted organization. The packages sometimes contained gifts along with the USB drive, like teddy bears and gift cards, meant to entice the recipient and bolster its validity. The detail of knowing who to address the packages to illustrate the deliberate act of targeting US personnel in positions with the placement and access to something FIN7 sought out. The USB drives contained GRIFFON malware, capable of espionage and destruction. FIN7's plan used social engineering to fuse the physical act of sending USB drives to specific recipients with the purpose of conducting a destructive remote, cyber-attack that would have been executed if any one of the recipients plugged them in.[62]

If an employee of the U.S. government received one of FIN7's packages, communicating it throughout the organization would reduce the chances of it working against them. It would most likely be reported to physical security given their presence and availability to employees compared to their cyber counterparts, who are often working outside of public view. Proper risk management activities would involve communicating every detail of the event to cyber security for the purpose of identifying the malware on the USB drive and taking the necessary

[61] Taylor Armerding. Synopsys, The cyber-physical convergence is accelerating and so are the risks. (2019)
[62] Ionut Ilascu, Bleeping Computer, FBI: Hackers Sending Malicious USB Drives & Teddy Bears via USPS. (2020)

precautions. After the details are analyzed, the organization may alter its security posture based on its new risk level. The factors that would influence the risk level are who it was sent from (the threat), what its intent was (the threat's will), who it was sent to (the organization's vulnerability), and what it could achieve against the organization (capability and impact). Additionally, passing the information to counterintelligence would prompt an investigation into why that specific employee was targeted, as encouraged by EO 12333.[63] Lastly, collaboration would enable the organization to broadcast the threat details to the entire organization for educational and warning purposes, which would increase the likelihood of other employees reporting suspicious behavior. Adhering to ISC's guidance, this information would also be shared with other organizations throughout the defense industry to reduce the risk of other agency's employees being compromised.

A real-world example of an attack against the government occurred in 2008, later named Buckshot Yankee, and was the catalyst for banning portable media devices in government facilities. A US Soldier found a USB drive in the parking lot of a base in the Middle East and plugged it into the network. The Soldier was unaware that the USB drive contained very malicious malware that eventually infected both the Nonsecure Internet Protocol Router and Secret Internet Protocol Routers of US Central Command. It took 14 months to recover from and eliminate the threat introduced by that USB drive and the exact damages have not been disclosed to the public.[64] It required an analyst from NSA to discover the threat and investigate to discover the network had been breached. The event was then communicated throughout the defense community so necessary precautions may be taken to prevent the spread. This is an example of

[63] National Archives. Executive Order 12333. (1981)

[64] Infosecurity-magazine.com/news/worm infosecurity magazine buckshot yankee

how risk management and security can work in harmony to better protect everyone. Unfortunately, it took a very damaging breach to occur before proper security policies were implemented, much like what happened after the Alfred Murrah building bombing in 1995.

## Security Risk Model

The following security risk model was published in the GSA's *Playbook: Enterprise Risk Management for the US Federal Government*. The GSA created the playbook to aid the ISC with implementing the risk management process throughout federal facilities. Therefore, it is the standard used by security and risk personnel at each federal organization when considering and planning for the protection of each building's systems and elements.[65] There are many other risk management models and processes, but this was created for integration into the government and the following sections will outline and discuss each step with real world examples. There are very minor discrepancies between other models, with the most significant being the emphasis placed on communication and analysis. The variance is likely due to the revenue driven nature of private industries compared to the national security focus of the government organizations using GSA's model. In many cases, risk management also differs in private industry because of the effect actions have on stock prices and the approval process of executive boards.

### Step 1: Establish Context

Within the U.S. government, the first step of security risk management is establishing risk context based on the facility security level (FSL), which is assigned to each federal facility. The FSL is derived from assessing risk factors such as mission criticality, symbolism, facility

[65] General Services Administration. ISC Risk Management Process. (2020)

population, facility size, threats to the agency, and any intangible factors.[66,67] The FSL sets a quantitative objective for security to achieve through their efforts. Critical to establishing context is determining what requirements and constraints influence the decision-making process of the organization's senior leaders. This may include policy concerns, mission needs, agency culture, and their unique risk appetite.[68] In establishing context, a baseline level of protection (LOP) will also be determined, which should be commensurate with its level of risk. There are 31 different threat scenarios used by risk analysts to determine the appropriate LOP, ranging from active shooters to arson.[69] The LOP then includes the specific countermeasures security will implement at the facility to meet the associated FSL. This practice stewards funding and operational decisions that influence the implementation of appropriate countermeasures. Without accurately understanding the FSL and LOP, federal organizations would be making uninformed decisions on their protection needs.

Based on the Washington Navy Yard's FSL, strict access control measures and a strong physical security posture were set in place, per the ISC's guidelines. Additionally, the Office of Personnel Management (OPM) conducted background investigations to determine every employee's eligibility to enter the facility based on suitability and fitness for duty. Background investigations are a crucial aspect of risk management, but are not a guarantee of future behavior as they only uncover information about the subject's past.[70] In the case of the Navy Yard shooting, the shooter had a criminal background with gun related incidents that would have prevented him from being employed if discovered during his investigations, his employer told

[66] Congressional Hearing. House Hearing 113, Facility Protection. (2013)
[67] Interagency Security Committee. The Risk Management Process for Federal Facilities. (2016)
[68] Chief Financial Officers Council. Enterprise Risk Management. (N.d.)
[69] Congressional Hearing. House Hearing 113, Facility Protection. (2013)
[70] Ibid.

the media.[71] However, the shooter had a pre-existing Secret security clearance that was granted by the Navy in 2008, despite that investigation uncovering his deception and omittance of previous criminal charges. Additionally, supervisors from both the Navy and his civilian employer claimed they were aware of his mental illness and deception on his background investigation, but it was never reported to the appropriate security clearance officials.[72]

This example highlights significant human errors that caused an extremely traumatic experience for many people, leading to the death of 12 Navy Yard employees. However, based on the facility's FSL and resulting security posture, the impact of the attack was less than it could have been. Part of the Navy Yard's LOP included armed Military Police and Security Officers, who created resistance for the shooter and restricted his freedom of movement, which likely reduced casualties.[73] While there was a clear failure in executing the security clearance countermeasures, overall the risk management process was successful at mitigating the risk by limiting the threats impact.

## Step 2: Identify Risks

The next step is identifying and assessing all hazards risk through continual analysis. Since risk is a product of threat, impact, and vulnerability factors, analyzing them and the associated conditions is the only way to accurately determine if the baseline LOP is enough or requires customization. Mitigating vulnerabilities to threats, through elimination or reduction, along with their potential impact is the objective of this process and accomplished through security's countermeasures. There are a variety of mathematical models and algorithms risk

[71] Karen McVeigh, Paul Lewis. The Guardian, Aaron Alexis Passes Recent Background Checks by Employer and Gun Store. (2013)
[72] William Henderson. Clearance Jobs, Aaron Alexis and the Failure of the Federal Security Clearance. (2013)
[73] Metropolitan Police Department. After Action Report, Washington Navy Yard. (2013)

practitioners may use to illustrate the impact of increasing protective countermeasures on the risk equation. These models are often used for quantitative risk assessments, which are highly effective at portraying numerical values of threats, vulnerabilities, and impacts. For security risk purposes, these are most valuable for specific risk assessments as the model can demonstrate how the countermeasures influence the LOP.

Identifying risks is often confused with threat identification. However, illuminating the threat landscape is only part of risk identification because it involves things that are not threats, such as poor training and toxic leadership. In the Navy Yard shooting, testing the security alarm may have resulted in a newly identified risk; the sound of the alarm's siren was too loud, causing sensory overload for responders and occupants of the building and severe degradation of their ability to communicate.[74] The extreme sound elevated the facility's risk level because of how it impaired the response capabilities and created a more dangerous environment. Preemptively identifying this and communicating it to those who needed to know would have enabled security to adjust the siren to a more appropriate decimal level before an incident occurred, which would have facilitated a safer and more efficient response.

### Step 3: Analysis and Assessments

Risk analysis is a process meant to assess the size and severity of risks, both individually and collectively, so appropriate countermeasures can be implemented. Risk assessments are a tool used to facilitate the analysis, and may involve facility audits, surveys, or evaluating specific concerns. Throughout the assessment process, risks are identified and categorized based on severity levels and probability. Organizations can then prioritize risks for mitigation once they

[74] Ibid.

understand the root causes, sources, and potential negative or positive outcomes. Then it becomes imperative for organizations to reduce their risk through allocating resources for their mitigation efforts. However, being too risk-averse may also be detrimental because of how that may lead to a misappropriation of personnel or finance resources when risk data does not support the associated actions.

There are two types of risk assessments, organizational and specific. Organizational risk assessments encompass the overarching organizational structure, resources, budget, employee commitment and account for the organization's mission.[75] An organizational risk assessment could be used to update senior leaders to ensure the organization's risk appetite is current and constantly followed. As a form of governance, any changes in the risk appetite would be immediately communicated through the security leadership to ensure security practices were aligned, thus further guiding the allocation of resources and financial planning purposes.

A specific risk assessment is tailored to an individual business unit or department and its unique objectives, not the strategic objectives of the organization. Conducting risk assessments provides analysts and leaders the information required to conduct thorough analysis based on a point in time under review. The act of analyzing a specific risk is considered a subcomponent of the dynamic risk assessment process, which are not always threat driven. It involves analyzing data to develop hypotheses and identify conditions of risk events, risk factors, and their potential substitutes. However, the result of any risk assessment can be qualitative or quantitative, depending on the needs and information of the organization. A qualitative risk assessment is

[75] American Society for Industrial Security. Guideline (GSRA): General Security Risk Assessment Guideline. (2015)

advantageous when historical data is not available, there are resource restrictions, risk factors are not fully understood, and management will better understand a descriptive presentation. A quantitative risk assessment is better for an organization when there is a general agreement on underlying assumptions, numerical scores can be used to describe risk factors, and enough data is available for the analysis.[76] Both kinds of risk assessments will describe conditions required for a risk event, the associated factors, and account for any cause and effect relationships. Risk assessments aim to answer the following questions: What can go wrong? What is the likelihood that it will go wrong? And what are the consequences if it goes wrong?[77]

To accurately answer the risk assessment questions, the first aspect of the required analysis is threat identification, which is determining all potential dangers and hazards, like an active shooter or cyberattack. Threat identification provides an opportunity to conduct analysis on the threat landscape, which is a collection of all individual threats to the organization. This makes the ISC's increased collaboration and timely sharing of intelligence vital for gaining valuable time and providing a more complete picture of the threat landscape, because it is possible for threats to be missed. Since the nature of every threat is to thwart countermeasures, the analysis of each individual threat is important for appropriate asset allocation and security-risk decision making.

Examining and understanding each threat's "capability" and "will" provides actionable insight for the risk and security managers to consider. In some cases, a threat is highly capable of a deadly attack, but lacks the will or motivation to execute it, which reduces its threat score. An example would be a disgruntled employee who wishes to harm fellow employees, but is

[76] American Society for Industrial Security. RA 1-20-2015. (2015)
[77] Andrew Blyth, et al. ScienceDirect, A Review of Cybersecurity Risk Assessment Methods for SCADA Systems. (2016)

incapable of obtaining a weapon to do so; their will alone makes them a threat, but their inability to obtain a weapon reduces their capability, and consequently their threat level. However, some threats are non-criminal, such as a labor strikes, power failures, and natural disasters, but they too must be considered and assessed when evaluating the threat landscape as security departments will have a role in responding to them as well. Aside from the practical considerations for a security program, understanding every possible threat is also used for insurance liability coverage and preparing for anticipated events.

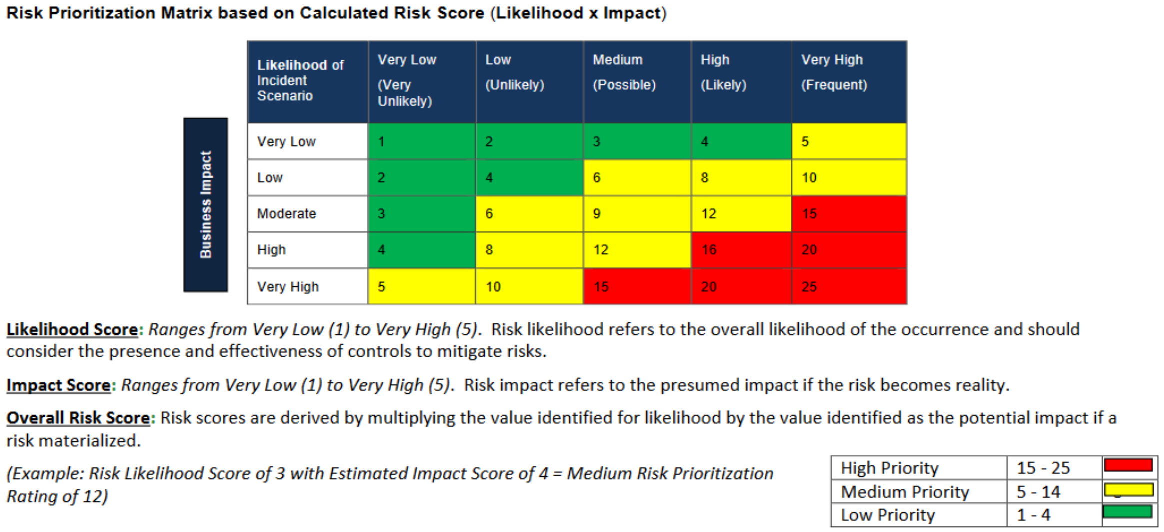
Another aspect of analyzing risk is identifying and evaluating internal vulnerabilities. An organizational vulnerability is any weakness that an aggressor could exploit, anything that could hinder the organization's response after an incident, or anything of value susceptible to damage from a threat. General vulnerability examples include single points of failure, ease of an aggressor to access an asset, or presence of valuable material, such as classified information or advanced weaponry as many federal security programs are charged with protecting. Physical vulnerabilities may include weak door locks, poor security policies, inadequately trained security personnel, or even poorly marked buildings that could delay first responders, which happened in the Navy Yard shooting.[78] Information, or cyber, vulnerabilities could include weak firewalls, a lack of paper shredders, poor password policies, or outdated security software. Maintaining an ongoing understanding of the organization's vulnerabilities enables it to also calculate the potential cost associated if a vulnerability is exploited.

The final aspect of analyzing risk is understanding the impact, or potential consequences, of a risk event. For impact to be fully understood, analysts need to completely understand the

[78] The District of Columbia Communications Interoperability Summit: A 6 Year Review of the Washington Navy Yard Shooting. (2019)

value of the assets they are analyzing and what would happen if they were compromised. Assets may be tangible, like buildings or people, or intangible like reputation or organic knowledge. The impact of a compromised asset may be calculated by direct cost, damage to the mission, or the potential for loss of life. To better understand consequences, impact models may be used as a tool for depicting possible outcomes. The information derived from the models can be used as data in quantitative risk matrixes, as pictured in Figure 1.0.

***THIS SPACE INTENTIONALLY LEFT BLANK***



**Risk Prioritization Matrix based on Calculated Risk Score (Likelihood x Impact)**

| | Likelihood of Incident Scenario | Very Low<br>(Very Unlikely) | Low<br>(Unlikely) | Medium<br>(Possible) | High<br>(Likely) | Very High<br>(Frequent) |
|---|---|---|---|---|---|---|
| Business Impact | Very Low | 1 | 2 | 3 | 4 | 5 |
| | Low | 2 | 4 | 6 | 8 | 10 |
| | Moderate | 3 | 6 | 9 | 12 | 15 |
| | High | 4 | 8 | 12 | 16 | 20 |
| | Very High | 5 | 10 | 15 | 20 | 25 |

**Likelihood Score**: *Ranges from Very Low (1) to Very High (5).* Risk likelihood refers to the overall likelihood of the occurrence and should consider the presence and effectiveness of controls to mitigate risks.

**Impact Score**: *Ranges from Very Low (1) to Very High (5).* Risk impact refers to the presumed impact if the risk becomes reality.

**Overall Risk Score**: Risk scores are derived by multiplying the value identified for likelihood by the value identified as the potential impact if a risk materialized.

*(Example: Risk Likelihood Score of 3 with Estimated Impact Score of 4 = Medium Risk Prioritization Rating of 12)*

| | | |
|---|---|---|
| High Priority | 15 - 25 | 🟥 |
| Medium Priority | 5 - 14 | 🟨 |
| Low Priority | 1 - 4 | 🟩 |

Figure 1.0

Source: DHS Risk Management Playbook (2016)

The physical construction of the Alfred Murrah Federal Building, in Oklahoma City, represents a poor or nonexistent impact analysis because of the weak steel chosen to build the structure, along with the absence of any access control measures. The Murrah building was attacked by a truck bomb that sheared off the front half of its structure because the steel melted from the heat of the bomb, which detonated at an ideal range for massive damage. In the example from Figure 1.0, the likelihood of a bomb detonating may have been awarded a numeric value of 3 because it was possible, but lacked threat indicators or data insinuating an eminent attack. However, the impact would have been rated "Very High," giving it a risk score of 15 and classifying it as a "High Priority" risk.

Estimating potential impact of compromised assets in conjunction with threat levels and vulnerabilities enables the analytic process to produce a security risk score. Since security risk scores are based on a consistent methodology, they establish priorities for where an organization is most at risk and needs to allocate additional security resources for mitigation and risk reduction efforts. The process of risk analysis enables risk management to build on the assessment's findings by answering another set of questions: What can be done and what options are available? What are the associated trade-offs in terms of all costs, benefits, and risks? What are the impacts of current management decisions on future options? Had risk management been a consideration in the Murrah building example, the high priority score of 15 would have warranted additional resources to reduce the score. If the assessment was completed pre-construction, it is highly likely stronger steel beams would have been selected to build the structure. Additionally, better access control procedures, like traffic bollards, would have been built to limit a vehicles proximity to the building, which would weaken a bombs effectiveness. The tradeoffs would have been an increased walking distance for employees and visitors along with more expensive construction materials in exchange for many lives. Unfortunately, the Oklahoma City bombing was the catalyst for many of the progressive security risk management practices used today, not just in government, but every industry.

## Step 4: Develop Alternatives

Driven by the organization's risk appetite, choosing response options, or strategies, for accepting, transferring, sharing, avoiding, or mitigating major risks is the next step in the risk management process. While also highly analytical, it is during this step that the cost of addressing the risk compared to the risk exposure will be considered and used for asset allocation decisions by senior leadership. It is middle management's job to provide control options, which may be preventative, corrective, directive, or detective in design.[79] The alternatives are selected based on the organization's mission, regulatory requirements, and available resources.

Risk acceptance differs from the other alternatives because it does little to reduce its effect. Instead, it is an acknowledgement and signifies that senior leadership is aware of the risk and believes it to be within their risk appetite. Accepting risk often occurs when the cost of other options, such as mitigation or avoidance, outweighs the risk itself.[80] Within the government, commanders and senior leaders decide to accept risks on a case by case basis, often based on the recommendations of their subordinates.

Transferring risk involves the contractual relationship of a third party, often an insurance company, that accepts responsibility for covering losses. Insurance exists as a means of transferring risk through a policy that covers certain events. Many regulations require very

[79] Chief Financial Officers Council. Playbook: Enterprise Risk Management for the U.S. Federal Government. (2016)

[80] Eric Conrad. ScienceDirect, Risk Acceptance. (2017)

specific insurance policies to meet compliance needs. However, the cost of insurance varies based on the level of risk they are being transferred through the policy. An example of risk transfer is workers' compensation, which is what prevents an employee from suing their employer for on the job injury or death. The family of a victim from the Navy Yard shooting sued the government for negligence because the Department of the Navy and the Department of Veterans Affairs failed to revoke the shooter's access after many warnings of his mental health issues.[81] They reached a monetary settlement five years after the case was filed, which was likely paid by insurance.

Sharing risk is like transferring it, but differs because there is no monetary exchange and it divides the total risk between two or more parties. Many of the federal mandates and regulations regarding security and risk management are an effort to share risk. Increasing collaboration and involving organizations such as the ISC and FPS are strong examples of risk sharing given the duality of efforts. However, it only applies to organizations working together to reduce risk, uninvolved third parties do not share risk directly.

Risk avoidance is a key element of risk management. It can be accomplished by not participating in activities that create risk factors or eliminating a risk event's chance of occurring. Security does a great job using risk avoidance at federal facilities by creating and enforcing prohibited items policies under 18 USC 930; many federal facilities prohibit employees from entering the workplace with 3+ inch long blade pocket knives, portable media devices, or alcohol.[82] Security screening of employees and visitors make these policies effective. Removing the prohibited items avoids their associated risk by eliminating the threat they pose.

[81] Kevin Gray. Reuters, Family of Victim in Navy Yard Shooting Sues U.S. for Negligence. (2013)

[82] Department of Homeland Security. FAQ Regarding Items Prohibited from Federal Property. (N.d.)

Lastly, “risk mitigation” is a general term used to describe the actions taken to reduce adverse effects.[83] This option is made possible by accurate analysis, but heavily executed by security programs. Security’s use of deterrence, response, defense, and investigative operations are all aspects of risk mitigation. Installing security cameras are an example of risk mitigation because it allows security personnel to monitor the safety of their facility without a physical presence. It is important that risk mitigation strategies match their organization’s risk appetite and unique mission objectives, which will be manifested into its security posture.

## Step 5: Respond to Risks

Responding to risk is an ongoing, multi-phased aspect of the risk management process. Like choosing a risk alternative, first assessing the organization’s risk is the only way to ensure an appropriate response. Based on the risk priority list, strategies are to be created and implemented to manage them. In some cases, risk response is exemplified through traditional security practices as they often prevent a risk occurrence. However, emergent threats require a more immediate response, such as additional security personnel, stricter access control measures, or added employee searches.

Choosing a risk response strategy is often done by senior leaders as they are the ones capable of approving the associated costs. Risk response can be a strategic, forward leaning approach meant to address a future risk based on something that will only threaten the organization later. Or, risk response can be an emergency when prior risk reduction or mitigation practices take effect and require immediate attention. The government’s response to the Buckshot Yankee breach involved cyber analysts first understanding the impact of the malware

[83] Xavier Franch, et al. ScienceDirect, Community Data for OSS Adoption Risk Management. (2015)

by tracing its steps. Only then was the NSA able to make recommendations based on what information was compromised and how it maneuvered through the networks. In the Navy Yard, security and law enforcement personnel responded by engaging the shooter directly and ultimately taking his life to eliminate the threat.

## Step 6: Monitor and Review

Through constant monitoring, risk information is acquired and must be reviewed to ensure the organization is still protected effectively. To do so, organizations must regularly review, monitor and update their risk registers to reflect any changes in their threat landscape or vulnerabilities. Risk reviews should occur semi-annually at a minimum and are meant to be an on-going process between security personnel and senior leadership.[84] Organizations benefit the most when risk reviews result in communication that highlights the status of risk response activities and actions because of the added awareness and reminder of their dedication to risk management. The risk communication may also include information on residual risk, milestone updates, or where additional response is required.[85]

## Step 7: Continuous Risk Identification and Assessment

[84] CFO Council. Playbook: Enterprise Risk Management for the U.S. Federal Government. (2016)

[85] Ibid

Lastly, the entire risk management model is meant to be an iterative process, constantly occurring, and requiring accurate analysis. However, the analysis is only as good as the available information, which is why continuous risk identification and assessments are necessary. As informative products, risk assessments can be living documents that evolve with new information or updated analysis. They are also meant to account for risk indicators internal and external to the organization, with collaboration being at the forefront of every risk endeavor. Building risk management into the workplace culture enables the organization to learn from and improve its processes from its managed risks, near misses, or any risk event that occurred.[86] Figure 2.0 shows Step 7 as a circular band, encompassing the previous 6 steps because it is vital to the organization's continued success with risk management.

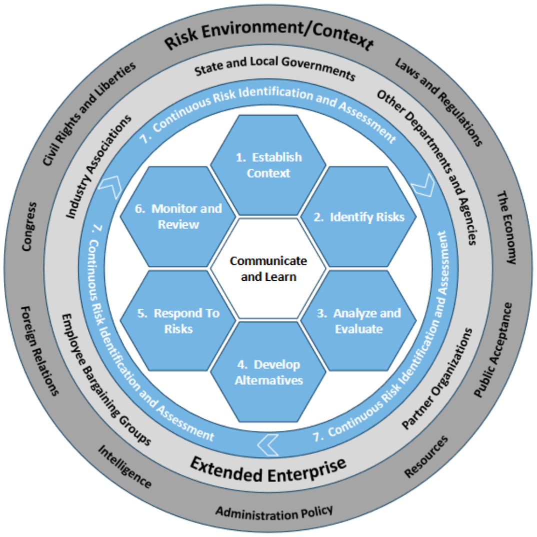


Figure 2.0

Source: https://cfo.gov//wp-content/uploads/2016/07/FINAL-ERM-Playbook.pdf

## Chapter 2: Conclusion

In conclusion, fusing risk management with security programs is a proven way to increase protection by reducing an organization's exposure to risk. It ensures that security programs are not standing still in a complex and fluid threat landscape. Its importance is evidenced by the fact that multiple executive administrations have mandated federal

[86] Ibid

organizations to make it part of their practices due to the assurances it provides. The EOs and circulars ensure senior leadership play a positive role in stewarding the risk management process. Additionally, communicating and building a strong risk-informed culture pays dividends by expanding awareness and generating pragmatic solutions. This is especially true in a federal setting where communicating risk and transparency is an expectation of the tax payers, relevant stakeholders, and Congress.[87]

Unfortunately, much of risk management's value in security was discovered through the analysis of great tragedies, such as the Navy Yard shooting and the Oklahoma City bombing of the Murrah Building. Thankfully, organizations recognize the need to evolve and have the help from government elements like the ISC. Through new policies and risk informed security practices, federal workplaces will find the protection they need to operate without interruption of violence or issues that disrupt their ability to continue protecting the country. While many of the civilian organizations seem to have evolved seamlessly, it appears as if the service components still have a lot of room to grow. Many of the guidelines disseminated by the DHS and the ISC articulate that they do not apply to military bases, leaving a significant vulnerability. This is potential evidence that the DOD is behind in this regard and supports the notion that FPCONs alone are not the most effective strategy to protect a base. Implementing risk-based security programs requires tremendous analysis, dedication, and effort, but is a worthy investment because of the potential to save countless lives. It is impossible to quantify exactly how many risk events are prevented by the risk model, but its integration with federal security programs undoubtedly makes federal facility workplaces much safer.

[87] Government Accountability Office. GAO-17-63, Enterprise Risk Management. (2016)

# Chapter 3: Insider Threat

When assessing an organization's threat landscape, external threats are often the focus of analysis. Unfortunately, the threat from within is increasing in prevalence, complexity, and jeopardizing national security. As the threat landscape continues to evolve, so too must the industries it indiscriminately victimizes. Currently, insider attacks occur most often in the healthcare, government, manufacturing, technology, and finance verticals. However, the focus of this thesis installment will be the impact to national security from insiders within the Department of Defense (DoD) and their associations with security and risk management programs, as discussed in the previous 2 chapters.

Insider attacks account for billions of dollars lost annually, in actual and/or potential lost revenue, as reported by ODNI, but how is the damage to national security quantified?[88] The complexity associated with answering that question lies within the organization's ability to capture events that never occur, as that is the nature of any ITP and makes their success extremely difficult to quantify. Insider threats are influenced by a combination of technical, behavioral, and organizational issues, which makes the overall threat incredibly complex and difficult to defend against when combined with each attacker's differing motivations. Insider attacks can include theft, violence, sabotage and can occur in both the physical and cyber domains. An organization can often detect or control when an outsider (non-employee) tries to access restricted data, either physically or electronically, and can more easily mitigate that threat from the damage they intend to cause. However, an employee with trusted access is more difficult to detect and, for that reason, can produce prolonged damage; a problem the U.S.

[88] DNI. Protect Your Organization from the Inside Out: Government Best Practices. (2016)

government contends with on a constant basis as cleared employees have regular access to information that "the unauthorized disclosure of could be expected to cause exceptionally grave damage to national security," as defined by section 1.1 of Executive Order (EO) 12356.[89]

Insider threat attacks will likely continue growing in complexity and frequency as foreign competitors seek to gain advantages over the U.S., both economically and in global power, making the government a lucrative and strategic target. However, insider attacks that involve a foreign adversary requires coordination between the attacker and the adversarial state, which is often for the sake of espionage. This makes insider threats not only a security issue, but also an area of focus for counterintelligence (CI), as discussed in the 2020 National Counterintelligence Strategy. Due to the complexity, rising frequency, and potential for catastrophic damage, the U.S. Government has made many mandates for how federal organizations protect against the threat, such as Executive Order 13857 and a national Task Force. Yet, security and counterintelligence programs are likely still understaffed and under-resourced, creating an exploitable opportunity for adversaries to use insiders against the U.S. government. Additionally, there is a glaring cyber knowledge gap between physical security practitioners, counterintelligence personnel, and the information security departments, as discussed in chapter 1. This thesis installment will clearly define what an insider attack is and how a breach from within jeopardizes national security. Case studies will be used to illustrate how different insider attacks broke down security practices, furthers the need for intelligence driven security programs, and how risk management played into each scenario.

## What is an 'Insider Threat?'

[89] Executive Order 12356 – National Security Information. (1982)

An ‘insider threat’ is defined by Carnegie Mellon University’s Software Engineering Institute as “the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.”[90] An insider may conduct violence, sabotage, and/or steal intellectual property/ national security secrets for personal gain, or that insider may be a “spy”—someone who is compromising information or products in order to benefit another organization or country. In some cases, insiders are not even organic employees, just contractors given temporary access to the victim’s workspace for a certain job. Examples often include commercial cleaning, outsourced security personnel/ technology, or information technology (IT) help, which was what Aaron Alexis did at the Washington Navy Yard prior to his violent insider attack.

While all insiders have the potential for catastrophic damage to national security, not all are intentionally harmful. There are two categories that differentiate the attackers – unintentional and malicious. There is little research explicitly focused on unintentional insiders, but some are a result of carelessness or accidents, which is a non-threat driven risk. Scholars at the University of Oxford attempted to address this research gap and their research attributed most accidental insider attacks to poor policy management. Their findings show that many incidents could have been prevented if their policies were better defined, less technical, and more properly disseminated among the employees.[91] The second contributing factor to accidental incidents is human error, which can encompass negligence, failure, misplacing sensitive items, or a lack of training.[92]

[90] Daniel Costa. SEI, CERT Definition of ‘Insider Threat’ - Updated
[91] ObserveIT. The Primary Factors Motivating Insider Threats. (2019)
[92] Ibid

In some cases, unintentional insiders are tricked, or are unwitting to their role in an attack. Cybercrimes and cyberespionage have made employees a target of their schemes, leading to human enabled-cyberattacks. An example of this occurred against the DoD in 2008 when a malware infected USB drive was likely left in an unsecured parking lot at a military base in Afghanistan. An unwitting and curious U.S. Soldier found the drive and plugged it into their workstation, which was in an access-controlled space, and gave the attacker access to everything on the DoD's Secret Internet Protocol Router (SIPRNet) and the Joint Worldwide Intelligence Communication System (JWICS); both are classified networks, with material ranging in classification from Secret up to Top Secret on JWICS. This breach was named Buckshot Yankee and took years to clean up. The malware propagated throughout U.S. Central Command's systems for approximately 14 months, making it the most serious breach of a classified network in history.[93] It is unclear (or classified) who the attacker was or how much sensitive information was compromised, but the breach likely provided an adversary valuable information on operations, sources, or war plans; all offering the enemy a marked advantage they could use to counter the DoD's efforts and take American lives in the process.

The details of the attack's origin, in 2008, are not certain, but it is reasonable to assume the service member did not mean harm and was unaware of the damage they would cause by inserting the drive. This implies that a foreign adversary planned to circumvent the access control and security measures by having someone with authorized access (an insider) unwittingly execute the attack on their behalf. The attack occurred during a time when bootlegged movies and video games were commonly passed between deployed service members on similar thumb drives as the one infected. So, the unintentional insider likely thought they would harmlessly

[93] Blake Stilwell. We Are The Mighty, The Worst Cyberattack in DoD History Came From a USB Drive. (2020)

discover some new entertainment, not provide an adversary with classified material that could be used against them. Buckshot Yankee was a seminal event because it highlighted significant vulnerabilities in security programs. The information ascertained from the event likely led to intelligence driven security decisions that DoD employees still adhere to, like the prohibition of USB drives in secure spaces.

More sinister than the unintentional insiders are their malicious counterparts. These are the insiders who knowingly and intentionally use their privileged access to cause harm. However, their motivations for attacking their employer and country often range between political objectives, extreme religious ideologies, emotional revenge, and/or financial gain.[94] Since DoD employees have regular access to classified information, their ability to conduct a lot of damage to national security is very prevalent. The DoD has been victim to a long list of malicious insiders who used their access to cause destruction, most noteworthy include Anna Montes, Bradley Manning, Edward Snowden, and Nidal Hasan.

Insider events are further categorized by the attack itself, most of which are malicious. The loss or degradation of organizational resources or capabilities is classified by the National Insider Threat Task Force as sabotage, which can involve information technology, vehicles, weapons, or anything necessary for the organization to achieve its mission.[95] Insiders can also conduct terrorism, which is defined by the Federal Bureau of Investigations as "violent, criminal acts committed by individuals and/or groups to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature."[96] Another insider attack is workplace violence, which shares the violent nature of

[94] ObserveIT. The Primary Factors Motivating Insider Threats. (2019)
[95] National Insider Threat Task Force. Mission Fact Sheet. (N.d.)
[96] FBI. What We Investigate. (N.d.)

terrorism, but lacks the external, often political, motivation. Workplace violence perpetrated by insiders can include verbal, written, or any physically aggressive threat or attack against others.[97] There has been a lot of research on workplace violence as it seems to be an increasingly common danger. Much of the research indicates the insiders are acting out of retaliation and/or suffer from mental illnesses.[98,99] Theft and fraud are additional malicious insider attack types, but given the national security focus of this thesis, espionage will be the final type discussed as it is the most common and damaging attack.

Many malicious insiders use their access to provide foreign intelligence entities (FIE) classified information, which is known as espionage and often becomes a far more complex game of smoke and mirrors as portrayed in the movies. There are volunteer spies, like Edward Snowden, who seek out a FIE due to personal motivations or objections. However, most espionage cases involve the FIE taking their time to recruit an agent, or 'spy', who uses their placement and access against the targeted organization. Like Carnegie Mellon's definition, the Department of Defense Directive 5240.06 (DODD 5240.06) defines this specific insider as "a person who uses their authorized access to DoD facilities, systems, equipment, information or infrastructure to damage, disrupt, operations, compromise DoD information or commit espionage on behalf of a FIE."[100]

There is often a robust recruitment process as FIEs cannot openly divulge their true intent to every potential recruit without being apprehended and prosecuted, or falling victim to a risky double agent operation. The recruitment of a spy first begins with spotting a potential recruit.[101]

[97] Cybersecurity & Infrastructure Security Agency). Insider Threat – Workplace Violence. (2020)
[98] Intelligence and National Security Alliance. Assessing the Mind of the Malicious Insider. (2017)
[99] Julian Barling. APA PsycNet, Preventing Insider-Initiated Workplace Violence. (2020)
[100] Department of Defense Directive 5240.06 (2011)
[101] Garret Graff. Wired, China's 5 Steps for Recruiting Spies. (2018)

This is where a foreign intelligence officer identifies a target using a variety of means, which now often includes social media, like LinkedIn or Facebook, where people often provide their employment information. Once spotted, the intelligence officer begins assessing the potential recruit for exploitable weaknesses, such as; extramarital affairs, gambling, drug addiction, and/or financial problems.[102]

The assessment may also include discovering potential motivators using the 'MICE' method – money, ideology, compromise, and ego, which could be used for coercion.[103] If there is any indication the FIE can exploit or coerce the recruit, they will move into the development phase, which is where they make contact and attempt to foster a close relationship. For their approach, the FIE's fake persona and background is often built in a manner that makes them most suitable to foster whatever kind of relationship they hope to establish with the recruit. The ensuing recruitment phase is the riskiest because this is when the FIE reveals the clandestine nature of their intent to turn the recruit into a spy, but often still uses deception regarding their strategic objectives and identity. The final stage is 'handling,' which involves the sensitive communication after the recruit has become a spy and is now disclosing national security secrets to the FIE, which is a national security crime punishable by death.[104]

It is extremely important to note that espionage has evolved in complexity due to the internet. Each phase of the cycle can be conducted without ever meeting in person, which makes detection and mitigation more difficult than ever. Additionally, human nature makes almost everyone susceptible to at least one of the MICE factors, but people are protected from being targeted by their potential motivators being concealed. Unfortunately, the internet unveils their

[102] DOD. DOD CI Awareness and Reporting Course. (2016)
[103] Randy Burkett. Cyberwar, An Alternative Framework for Agent Recruitment. (2013)
[104] Britannica. Federal Capital Offenses. (2012)

shroud of privacy and enables FIEs to build an approach plan tailored to their target's unique circumstances; complements of hackers' ability to illicitly obtain sensitive information, as evidenced by the OPM data breach in 2015.

To reduce the likelihood of insiders operating within the government, there are many countermeasures used to prevent and discover them. The first countermeasure is the pre-employment polygraph, often used by defense agencies before granting security clearances. The polygraph is a counterintelligence function, illustrating another example of intelligence informs security by determining if employment candidates are trustworthy. Additionally, most federal agencies mandate current employees retake a polygraph every five years, which is meant to discover if an employee has become compromised and it potentially an insider. Another countermeasure provided by intelligence to discover insiders is user activity monitoring (UAM), as discussed in chapter 1. UAM is effective because federal employees all agree to consensual monitoring while accessing government networks as a requirement of their job. Per Executive Order 13587, UAM is required to counter insider threats by monitoring for suspicious activity, such as nefarious communications or removing classified information from a system.

Insider espionage imposes a tremendous cost on the DoD and national security in terms of strategy loss, the potential for lost lives, and significant monetary expenditure. However, insider-spies do not directly conduct violence against their fellow employees, as they are likely motivated for financial benefit or coerced by something discovered in the assessment phase. Unfortunately, FIEs are not the only foreign groups targeting insiders; international terrorist organizations (ITOs) use similar methods to recruit people sympathetic to their causes. When deep ideologies become motivation for betrayal and extremist action, radicalization and violence are likely to ensue. To the detriment of national security, ITOs also use the internet and are capable of mobilizing insiders without ever meeting in person.

In 2009, U.S. Army Major Nidal Hasan fatally shot 13 people and wounded 32 others, at Ft. Hood, TX, in a vicious act of 'lone wolf' terrorism.[105] Hasan was a trusted field grade officer in the Army, serving as a psychiatrist to Soldiers and their families. His attack was religiously motivated, yet his cousin described him as less of a devout Muslim at one time, who more so practiced his faith culturally.[106] However, life circumstances prompted a religious intensification that radicalized and motivated him to kill his fellow Soldiers, making him a malicious and extremely violent insider.

Hasan's radical departure from peaceful religious beliefs is likely attributed to three major factors, which played out in a linear progression.[107,108] The first being family; Hasan's mother died in 2001 and he was worried that her spiritual life, while alive, would not earn her soul a place in heaven. She began practicing Islam more devoutly in the later years of her life, but Hasan was most concerned because she, and his father, owned a convenience store that sold alcohol, which is forbidden by Islam. To redeem his mother, he believed any 'good actions' he did on her behalf would outweigh her sins, as sort of a "religious karma" he began to believe in during the initial stages of his radicalization.[109] In pursuit of a more devout life, Hasan also began searching for an appropriately pious wife.[110] However, no potential spouses ever met his standards in beauty or Islamic views.[111] His interpretation of Islam was largely derived from

[105] Katherine Poppe. George Washington University, Nidal Hasan: A Case Study in Lone-Actor Terrorism. (2018)
[106] Ibid.
[107] Clint Watts. Foreign Policy Research Institute, Major Nidal Hasan and the Ft. Hood Tragedy. (2011)
[108] Katherine Poppe. George Washington University, Nidal Hasan: A Case Study in Lone-Actor Terrorism. (2018)
[109] Ibid.
[110] Ibid.
[111] Clint Watts. Foreign Policy Research Institute, Major Nidal Hasan and the Ft. Hood Tragedy. (2011)

researching very radical and intolerant Islamic scholars, such as Sayyid Qutb (the same scholar who inspired Osama bin Laden) and Anwar al-Awlaki, who was a known al-Qaeda member.

The timing of his mother's death in conjunction with the 9/11 terror attacks created an extremely vulnerable time period for Hasan, which is the next factor in Hasan's radicalization. While still grieving the loss of his mother, Hasan's research pushed him toward a tremendously conservative brand of Islam preached at the Dar al-Hijrah mosque in Falls Church, VA. The mosque was widely known for its attendance by two of the al-Qaeda terrorists, who hijacked airplanes on 9/11, and its preacher, Anwar al-Awlaki, the extremist Islamic scholar Hasan had been researching.[112] After the 9/11 attacks, al-Awlaki gave a sermon that equated the war on terror to a global war against all Muslims, which took root in Hasan. His devotion to the mosque initiated an ideological introduction with al-Awlaki that would later play into his attack at Ft. Hood.

Eventually Hasan became a psychiatrist and worked with troubled Soldiers who returned from the conflicts in Iraq and Afghanistan. Their stories of horror and revulsion took an emotional toll on Hasan as he battled an internal affliction. His work trying to help the emotionally battered Soldiers led to an intense fear about deploying, which is an obligation most Soldiers willingly accept. In addition to the fear his counseling work instilled in him, he was overtly, morally opposed to the wars he was expected to serve in. It was later disclosed that Hasan's sentiment toward the war was evidenced in his writings and decaying relationship with his family, which should have served as strong indicators of potential violence.

[112] Ibid.

Hasan eventually received orders for a deployment to Afghanistan, which was the final catalyst in his linear radicalization. The deployment likely accelerated the timeline for the attack as he perceived it was a "task from God to speed up his [pending] actions."[113] In the year leading up to the attack, Hasan communicated with Anwar al-Awlaki nearly 20 times through the messaging function on the mosque's website. He sought information on when it was appropriate to conduct jihad, suicide, and God's expectations of him. Hasan contemplated conducting his attack while deployed, but ultimately decided to execute it in the Soldier Readiness Center, on base, because it was a building that he was familiar with; a familiarity gained through his authorized and regular access as an insider. After the attack, it was discovered that Hasan felt he was risking eternal condemnation to hell if he did not commit the attack, because he believed God commanded it. Hasan's communication with al-Awlaki prompted a federal investigation, albeit the FBI's Washington Field Office eventually dismissed as they could not conclude he was involved in terrorist activities.[114]

It is noteworthy that the FBI was aware of Hasan's communication with to al-Awlaki and his offers to conduct terrorism if needed. Hasan's progressing radicalization was also evidenced by many papers he wrote where he tied in his extremist beliefs. One of Hasan's classmates commented, "Hasan wore his rigid Islamic ideology on his sleeve and wove it through his course work…he would be standing there in uniform pledging allegiance to the Koran."[115] Given the evidence provided in hindsight and the fact that the FBI was aware of Hasan's radicalization, it is reasonable to assume this insider attack could have been prevented with better risk management and security practices.

[113] Katherine Poppe. George Washington University, Nidal Hasan: A Case Study in Lone-Actor Terrorism. (2018)
[114] Congressional Hearing. House Hearing, 112 Congress, Lessons from Fort Hood. (2012)
[115] Katherine Poppe. George Washington University, Nidal Hasan: A Case Study in Lone-Actor Terrorism. (2018)

As a violent insider, Hasan was motivated by religious ideologies. He is considered a volunteer as no one coerced him into committing the attack. He willingly sought out al-Awlaki's counsel and followed a very linear radicalization. His knowledge as a military officer at Ft. Hood enabled him to plan and execute his attack in a manner that accomplished his goal. During the attack, he deliberately avoided areas where his weapons could harm civilians as he believed harming Soldiers only was his God's intent. An external attacker would have likely been thwarted by security countermeasures and/or not had the foresight to know the demographics of each area as well as Hasan. Instead, he used intimate knowledge of knowing where there was a high concentration of Soldiers, who also were preparing for deployments to what he believed was a war against all Muslims, making it additionally symbolic for him.

## Insider Threat to National Security

The lives lost at Ft. Hood, during Hasan's insider attack, represent the tragic reality of how varying world views often collide with fatal consequences, but what are the strategic implications? Some insiders have the ability to degrade national security on a level many media viewers and mourners will never understand. The potential to not see beyond the crimes committed is often due to the concept of 'national security' being widely ambiguous and based on varying perspectives from strategic competitors. Whilst describing asymmetric warfare as a counter-balancing of force, David Grange stated, "Combatants throughout the ages have continually sought to negate or avoid the strength of the other, while applying one's own strength against another's weakness."[116]

[116] "David Grange, "Asymmetric Warfare: Old Method, New Concern," National Strategy Forum Review. (2000)

ScienceDaily defines ‘national security’ as, “the requirement to maintain the survival of the state through the use of economic power, diplomacy, power projection, and political power.”[117] This definition does not offer specifics, but infers unchallenged sovereignty and supports Harold Lasswell’s belief that national security means freedom from foreign dictation.[118] Unfortunately, many near peer threats aim to weaken each facet of the U.S.’ national security and insiders play an integral role in that. Economics, diplomacy, and military/political power represent the strengths and weaknesses Grange described as tenants of competitive strategy, each under constant attack.

To corroborate definitions and frame the rest of this research, President Donald Trump’s 2020 National Security Strategy (NSS) defines his strategic vision as “protecting the American people and preserving our way of life, promoting prosperity, preserving peace through strength, and advancing American influence in the world.”[119] To accompany the NSS, the Office of the Secretary of Defense (OSD) publishes a National Defense Strategy (NDS) that outlines how its federal organizations will accomplish the administration’s national security objectives. The NDS serves as the guiding policy for DoD organizations to adhere to and base their strategies on.

The OSD’s most recent NSD highlights a numeric “2+3 framework” prescribing the strategic priority of challenges threatening national security. The “2” represents OSD’s primary challenges; China and Russia, based on their strategic objectives combined with capability and will to displace the U.S. globally and their potential impact on national security. The following “3” represent the Democratic People’s Republic of Korea, Iran, and international terror organizations/violent extremist organizations (both meaning terrorist groups like al-Qaeda and

[117] ScienceDaily. Reference Terms, National Security. (N.d.)
[118] Lance Kent. The Australian Quarterly, Review: National Security and Individual Freedom. (1951)
[119] National Security Strategy. (2017)

ISIS, the differences lies in the groups' global presence).[120] Understanding the 2+3 prioritization framework is important because it signifies where defense resources are most likely to be allocated.

Each of the 2+3 benefit from having insiders within the DoD. As evidenced by Hasan, even ITOs can use insiders to further their ideologies, which certainly goes against the national security objectives of preserving prosperity and peace. Through self-radicalization and remote interaction, al-Qaeda benefited from one of the Army's greatest strengths (its Soldiers) turning into a weakness, in the name of their cause. The other 4 can impose their foreign influence on the U.S. and degrade the way of life mentioned by President Trump in his NSS. Additionally, they undermine the U.S.' economy while simultaneously decreasing global power through insider industrial espionage campaigns against cleared defense contractors (CDCs), like Raytheon and Lockheed Martin. Targeting CDCs is a tactic used to learn about the U.S.' equipment and technology, for the sake of being able to gauge lethality and plan countermeasures. The information FIEs seek varies by each nation's strategic objectives and their relationship with the U.S., which also equates to how aggressively they attempt to collect it. The desired targets of defense information of interest likely include all classified information, locations of sensitive information, technology, security vulnerabilities at cleared facilities, and personnel weaknesses that may be exploited, as mentioned in the recruitment process.[121]

Once the sensitive information is acquired, FIEs provide their nation's leadership the ability to make strategic policies and decisions that harm the U.S. and its interests. It also enables them to corrupt U.S. intelligence collection, which manipulates and distorts the U.S.' picture of

[120] U.S. Secretary of Defense. National Defense Strategy. (2018).
[121] DoD. DOD CI Awareness and Reporting Course. (2016)

reality used by senior decision makers to develop foreign policy and plans. The collective mediums used to ingest information is known as the information environment (IE). Data flows throughout physical, information, and cognitive domains, making up the complete IE. Manipulating the IE, in any way, is a devasting form of deception, or influence operations, that weakens each state's ability to allocate resources, plan conflicts appropriately, hold unadulterated elections, and distinguish between friend and foe. The information insiders provide FIEs serve as pieces of a proverbial information puzzle for the adversaries to use against the U.S. Knowing how the U.S. collects information, uses it, and what they are planning proves invaluable to adversaries who are likely disadvantaged militarily.

The outcome of a FIE obtaining defense information can be catastrophic. To counter the effects, the U.S. Government has many programs and policies in place for securing it, such as: strict classification guidance, robust security programs, risk driven decision making, and cutting-edge technology. However, the use of insiders to thwart those countermeasures has been successful in the past. As a result, many covert operations have been compromised by sources being revealed, which diminished the intelligence community's (IC) ability to collect against intelligence targets that saved American lives.[122] Special operations missions have been compromised, placing American troops overseas in grave danger. Newly created technology that was made to create a tactical advantage on the battlefield, and often cost millions to create, is made obsolete when the adversaries learn classified aspects of it. Each piece of information the FIE gains, is something the U.S. must recover from and mitigate the damage of its effects. The

[122] U.S. House of Representatives. Review of Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden. (2016)

complexity with this is that it is not always clear what information is compromised, or who received it.

The DoD and IC regularly reviews and attempts to assess the full scope of damage caused by insider threats, such as Edward Snowden, and those efforts can be quantified in the billions it costs to just conduct the review of leaked information. The money spent on the reviews does not include cost to technology, operations, or anything else. However, truly quantifying the intangible impact insiders have on national security is impossible. The metrics used to quantify damage include who the information goes to, such as the 2+3, and how/if the information is used against U.S. interests.

## Case Study: Edward Snowden

The infamous case of Edward Snowden releasing troves of classified information to the public and 2+3 adversaries perfectly represents the damage insider threats have on national security. He used his access as a contractor for the National Security Agency (NSA) to stealthily obtain and disclose massive amounts of damaging, classified information to the public and the U.S.' most strategic adversaries. The controversy surrounding Snowden results from him presenting himself as a noble 'whistle blower' attempting to protect civil liberties, not as a malicious insider. However, many in the media seemed to have a vested interest in protecting Snowden's image because  he initially met with two particular journalists, in covert fashion, to distribute his illicit information for their benefit.[123] However, open source research strongly suggests that he failed to report his concerns within the procedures clearly defined in the

[123] Amanda Holpuch. The Guardian, Journalists Who Broke NSA Story in Guardian Dedicate Award to Snowden. (2014)

Intelligence Community Whistleblower Protection Act of 1998, which enables members of the IC to raise classified issues in a manner that protects the employee and national security.[124] Additionally, all of the agency's activities were "authorized by two different presidents, from two different political parties, by Congress and by seven different judges, 16 different times," said NSA Deputy Director Richard Ledgett.[125] Therefore, this case study dismisses the 'heroic' whistle blower façade and will use Snowden to exemplify how insiders damage national security while exploring potential indicators that may have warned employers of what he would become and how his attack influenced risk management reform.

In 2004, young Edward Snowden was inspired to fight alongside the U.S. Army's elite Green Berets, so he enlisted as an 18X, which is a Special Forces candidate.[126] The road to earning the coveted green beret is arduous, but Snowden failed out of basic training due to shin splints, disqualifying him from ever coming close to the initial training and qualification courses the elite endure.[127] His reason for exiting the Army is significant because Snowden reportedly lied after the fact, often claiming he "broke both of his legs", using supposed injury as a honorable justification for his release. However, shin splints are not broken bones and this potentially small lie speaks to his integrity and propensity to exaggerate facts for perseverance of his self-righteous image, which has severe consequences for national security later in his career.

After leaving the U.S. Army, Snowden worked as a security guard at the University of Maryland's Center for Advanced Study of Language. As a condition of employment for this job, he was required to obtain a high-level security clearance and pass a counterintelligence

[124] U.S. Congress. Intelligence Community Whistleblower Protection Act of 1998. (1998).
[125] Sune von Solms. North-West University, The Consequences of Edward Snowden NSA Related Information Disclosures. (2015)
[126] Stephanie Gaskell. Politico, Snowden Lasted 5 Months in Army. (2013)
[127] Charlie Savage. The NY Times, House Intelligence Committee Urges No Pardon for Edward Snowden. (2016)

polygraph as the language center was owned by the NSA.[128] Exaggerating his injury as explanation for washing out of the Army was an early indicator Snowden's character was developing as someone who often failed to complete things he started and lie about them after the fact. As additional evidence of this, Snowden reportedly lied about graduating high school; he often claimed to have earned a GED, but a federal investigation after his breach proved otherwise, making his entire enlistment in the Army and future jobs based on false pretenses.[129] For his job application to NSA in 2012, his resume stated he graduated from Maryland High School in 2001. However, by Snowden's own admission on a public web form, he contradicted his resume and stated, " …[he] did not have a degree of ANY type. I don't even have a high school diploma."[130] Despite not even completing high school, he began classes at a community college in MD, which he also deceived, while he looked for other jobs. This deception likely added a layer of credibility to his false claim about completing earlier education as it is a prerequisite.[131] Alas, he attended a job fair in 2006 and got a job as a contractor for BAE systems at the Central Intelligence Agency (CIA). He worked in that position for less than a year before converting to federal civilian employee at CIA. His opportunity and service at the CIA led to extensive computer and tradecraft training that ultimately propelled his career in a direction that would give him access to the government's most closely guarded secrets. However, he was not a "senior advisor" for the agency, despite his claims of serving in such a prestigious role.[132]

[128] Oliver Darcy. Campus Reform, University of MD Won't Say if NSA Operates Secret Facility on Campus. (2013)
[129] U.S. House of Representatives. Review of Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden. (2016)
[130] U.S. House of Representatives. Review of Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden. (2016)
[131] Tal Kopan. Politico, 10 Things to Know About Snowden. (2013)
[132] U.S. House of Representatives. Review of Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden. (2016)

Snowden's service at the CIA was ultimately short-lived and riddled with employment concerns where he alleged discrimination, which began in his initial training. He often reported issues regarding "morale and retention issues" to his supervisors, but was dissatisfied with their response to his claims.[133] As a means of raising his concerns higher and hoping for a different outcome, he sent them directly to one of the ten most senior officials at CIA, but again to his disappointment. Upon completion of his training, he was assigned to an overseas billet. At one point during his time in that role, his supervisor claimed, he "often does not positively respond to advice from more senior officers, ... does not recognize the chain of command, often demonstrates a lack of maturity, and does not appear to be embracing the CIA culture…".[134] Despite not excelling in his duties and only serving in the position for a few months, Snowden asked to apply for a more senior role within the CIA. Ultimately, the same supervisor who did not express a lot of faith in Snowden refused to endorse his application and he was denied. As a result, he began another controversy with senior leadership over their ethics and hiring practices. It is also alleged that he modified his performance evaluation in CIA's performance review software, which resulted in numerous negative counseling sessions and a fitness for duty investigation, which happens when an employee's capability to perform is called into question.[135]

Snowden eventually resigned from the agency in 2009 due to alleged moral obligations about an operation he observed in Geneva. Snowden claimed the CIA set up a Swiss banker to be arrested for drunk driving by local police, which would cause significant trouble for the banker. Snowden's alleged intent for the CIA engineering the situation was for the purpose of gaining

[133] Ibid.
[134] Ibid.
[135] Ibid.

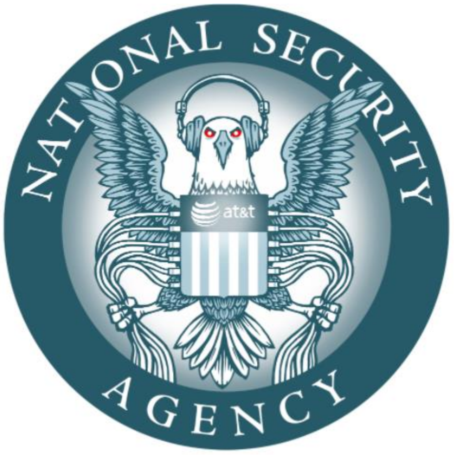
leverage over him, which they would do by offering to use their influence to have the charges dropped in exchange for his cooperation.[136] This was reportedly an operation to implicate Switzerland in U.S. tax evasion crimes, yet investigating international tax crimes is not likely an area of focus for the CIA based on a significant amount of open source research and the fact that they are not even a law enforcement/investigation organization. While Snowden was only 23 years old at the time, his allegation of illegal government operations was another strong indication of what he would become as none of his moral qualms were documented in any of the numerous complaints he filed during that period. It is feasible that his story of CIA wrong doing was just another false justification for his exit from the CIA.

An investigation into Snowden's Switzerland claim may have identified an integrity-based vulnerability that would have likely prevented him from gaining the future access he eventually earned at the NSA. However, if his claim was true, he could have reported it through the IC Whistle Blower Protection Act, which would have launched an investigation into the operation in question and likely made an impact if there was wrong doing, while affording him protection. Instead, Snowden opted to just quit as some sort of self-righteous act of heroism without any corrective action for the alleged ethics violation committed by the U.S. government. To support the likelihood that his claim was a falsehood, evidence suggests Snowden's position in the CIA would not have even provided him access or knowledge of such operations, again indicating he was a serial fabricator.[137,138]

[136] Reuters, Swiss President Would Back Criminal Probe against NSA Leaker. (2013)
[137] Ibid.
[138] U.S. House of Representatives. Review of Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden. (2016)

After leaving the CIA, Snowden got a job at Dell managing computer systems and doing cyber security for various government organizations. For Dell, he was initially assigned to an NSA contract in Tokyo where he was tasked with defending their networks from China. As a requirement of employment, Snowden had to pass an entrance test for NSA. It is widely reported that he hacked a database and stole the answers to the entrance exam, again exposing his true nature as an unethical cheater. His exposure of government operations was a flagrant security violation that should have had him permanently banned from further access to classified information, yet open source reporting does not provide any evidence that there was even an investigation over the issue. Albeit, Snowden was eventually promoted within Dell and given additional access to classified information. This security violation and the substandard response perfectly exemplifies a failure between counterintelligence and personnel security.

Figure 1.0



Source: https://www.dailydot.com/unclick/snowden-eff-hoodie/

Another strong indicator of his compromise was later reported by one of his coworkers; he often wore a black hoodie with an NSA logo parody, pictured in Figure 1.0. The logo used the eagle pictured in NSA's logo, but added headphones and showed it clutching cables hooked up to an AT&T cable box. This was meant to signify that NSA had a secret interception room in a San Francisco AT&T office, which was classified information and made his creation of this hoodie another security violation.[139] The inference of classified information on his sweatshirt was part of the information he later leaked. Had his co-

[139] Kevin Collier. Daily Dot, This hoodie Snowden was Wearing probably Should've Tipped off the NSA. (2020)

workers at NSA reported his hoodie earlier, perhaps another security investigation would have been conducted and revealed enough to seize his access.

In 2011, Snowden returned to Maryland, where he grew up, and began working on a CIA account for Dell. This was likely when he began illegally downloading and archiving classified material, but why would anyone do that if they were not a threat? Each time he illicitly ex-filtrated classified information, he committed security violations that should have prohibited his future access, yet security failed to learn of his intent, despite the numerous indicators leading up to this point. Eventually, he was reassigned again to another NSA site in Hawaii, but quit in 2013. He claimed his resignation was a result of seeing the Director of National Intelligence, James Clapper, committing perjury under oath during a Congressional testimony.

Snowden later claimed Clapper's dishonesty under oath was his "breaking point," insinuating that was the catalyst for him eventually becoming an insider threat. Although, the evidence proving he began downloading classified information prior to Clapper's testimony makes that appear to be another lie. Additionally, it is well documented that Snowden was repeatedly counseled for his behavior at work. He engaged in disrespectful email arguments with managers and senior leaders at NSA, initiated by his inability to pass annual basic training on Section 702 of the Foreign Intelligence Service Act just weeks before he quit.[140] His employment issues at both the CIA and NSA indicate a pattern of volatile behavior and an inability to meld with the workplace cultures, likely making him feel like a targeted outsider. Since retribution is a motivator for many insiders, it is plausible that he anticipated a hostile exit and began preparing

[140] U.S. House of Representatives. Review of Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden. (2016)

for his attack by collecting the classified information ahead of time, then used Clapper's false testimony as another self-righteous way of disguising his true reason for quitting.

## Snowden's Impact on National Security

For the explicit purpose of gathering damaging classified information, Snowden sought out employment with Booz Allen Hamilton, a cleared defense contractor who performs sensitive work for the IC.[141] From the onset of his new job, he began collecting and archiving classified data that he planned to release. The exact amount of classified information he collected and ex-filtrated varies, but was likely millions of documents. The information he stole pertained to sensitive operations the U.S. government was conducting and the surveillance operations and technology used against its adversaries. Additionally, the information included classified presidential orders to intelligence officials outlining cyber targets, which included foreign government officials and civilians. [142] The information he released mostly included information outside of what should be considered privacy infringement concerns for Americans, making nearly everything else an additional strain on foreign relations and national security.

In September of 2016, the U.S. House of Representatives released an executive summary after an exhaustive investigation into the Snowden breach. While not a direct impact on national security, it is important to note that the two-year long investigation into Snowden's damage likely cost millions of U.S. tax payers' dollars. The executive summary stated, "Snowden caused tremendous damage to national security, and the vast majority of the documents he stole have nothing to do with programs impacting individual privacy interested –instead, they pertain to

[141] Huffpost. Snowden Sought Booz Allen Hamilton Job to Gather NSA Surveillance Evidence. (N.d)

[142] Paul Szoldra. Business Insider, This is everything Edward Snowden revealed in one year of unprecedented Top-secret leaks. (2016)

military, defense, and intelligence programs of great interest to America's adversaries."[143] The exact effects on national security from his leak are clear; Chairman Mike Rogers stated, "Snowden's actions are likely to have lethal consequences for our troops in the field," portraying the severity of the leak for service members. Additionally, they provided the 2+3 adversaries vital secrets to the U.S.' success against them. The trove of classified information he released went directly to terrorists and near peer adversaries who are now capable of training and planning with a clearer understanding of the U.S.' capabilities, in terms of tradecraft, sources, and intelligence methods. "What we've seen the last six to eight months in an awareness by these [terrorist] groups…of our ability to monitor communications and specific instances where they've changed the ways in which the communicate to avoid being surveilled or being subject to our surveillance tactics," said National Counter Terrorism Center (NCTC) Director Matthew Olsen.[144] As a result, the operations used to safeguard U.S. sovereignty, foreign diplomacy, and military power were compromised and now the U.S. must play catch up and establish new programs and technologies to regain its ability to intercept terrorist communications.

There have been at least ten damage assessments conducted by various organizations and branches within the U.S. government and mostly all the findings are highly classified. The executive summary redacted and released by Congress provides the clearest insight into the actual damage. However, Joel Melstad, a spokesperson for the counterintelligence center claimed damage has been observed and verified in five categories of information, which the government keeps classified.[145] Melstad also affirmed the notion that each Snowden-disclosed documents compound the damage to national security; most likely in the sense that it exposed tools used to

[143] U.S. House of Representatives. Review of Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden. (2016)
[144] James Meek, et al. ABC News, Intel Heads: Edward Snowden Did 'Profound Damage' to U.S. Security. (2014)
[145] Deb Riechman. AP, Costs of Snowden Leak Still Mounting 5 Years Later. (2018)

amass intelligence and operations, put U.S. personnel and facilities at risk, and greatly destabilized U.S. partnerships abroad.[146]

Unfortunately, Snowden's impact on national security did not only harm the U.S. and its interests. Many of the Snowden-leaked documents implicated the United Kingdom and its ability to successfully achieve national security and diplomacy. As an example, Prime Minister David Cameron demanded newspapers stop publishing leaked NSA files about the UK's Government Communication head quarter's program that collected signal intelligence on Europeans. This specific leak caused strained relations between Germany, the U.S., and the UK as it was determined that German Chancellor, Angela Merkel's, phone was tapped as part of this combined operation.[147] As a result, the U.S. embassy, in Germany, faced great scrutiny and the alliance with Germany was weakened.

The international relations issues did not stop in Europe. The Brazilian government publicly expressed significant dissatisfaction after Snowden's leak revealed the NSA was spying on communications of senior Brazilian leaders. Brazilian President, Dilma Rousseff, was "furious" and demanded a public apology from the U.S. as Snowden revealed that the NSA was intercepting her private communications.[148] Additionally, Rousseff canceled a scheduled White House visit and downgraded commercial ties between the two nations. The Brazilian government was so outraged by Snowden's disclosure that they cancelled a $4.5 billion dollar contract with U.S. owned Boeing and gave the fighter jet contract to a Swedish company that they was more trustworthy.[149] This fractured diplomatic relationship happened at a time when the World Cup

[146] Ibid.

[147] Sune von Solms. North-West University, The Consequences of Edward Snowden NSA Related Information Disclosures. (2015)

[148] Brian Winter. Reuters, Exclusive: Brazil's Rousseff Wants U.S. Apology for NSA Spying. (2013)

[149] Alonso Soto. Reuters, Saab Wins Brazil Jet Deal After NSA Spying Sours Boeing Bid. (2013)

was about to occur in Brazil, which likely impacted the coordination of emergency response and prevention preparedness for security threats at the global event.

International terrorists often use commercial services, like Google and Yahoo, to communicate their plans. This makes commercial services a pivotal platform for collecting critical information used to defend against their attacks. This was another aspect of national security damaged by Snowden as his leaks antagonized relations with many large private data companies. Part of what he revealed was that NSA programs, used to counter terrorist plots, intercepted data from Google and Yahoo user accounts. This outraged both company's general counsel and ultimately caused them to extend their encryption across more platforms, making it more difficult for the NSA to collect valuable national security information.[150] Additionally, public outing revealed a crucial aspect of the intelligence community's playbook, which allowed terrorists to alter their communication methods in a manner that would be more difficult to intercept.

There is a strong possibility that the media painting Snowden as a patriotic hero, instead of reporting his true character, could have significant consequences in the future. It encourages others who may have ethical qualms about their intelligence work to follow a similar path instead of reporting their issues the correct way. Plus, the false narrative that Snowden is a hero creates added controversy over the government's ability to prosecute him and may impact future whistle blowers' willingness to come forward with legitimate issues. In addition to the national security damage he caused, U.S. technology companies were forced to spend billions building business centers in other countries to regain the trust that was lost after Snowden's breach. Yet,

[150] Sune von Solms. North-West University, The Consequences of Edward Snowden NSA Related Information Disclosures. (2015)

this furthers the potential for future damage as operating international business centers puts intellectual property in increased danger of being compromised. It is also highly likely that Snowden has not yet released all the information he obtained, making it nearly impossible to predict future consequences.

## Case Study: Security Failures

Education and employment verification are basic tenants of federal pre-employment background screening, making Snowden's high school deception an oversight that should have been discovered. Snowden would have been required to obtain a secret security clearance prior to joining the Army and then a Top Secret for his other jobs. For his background investigation, a Standard Form 86 (SF-86) would have been completed and submitted to OPM. Per the National Bureau of Background Investigations (NBIB), the SF-86 is "is a permanent document that may be used as the basis for future investigations, eligibility determinations for access to classified information or to hold a sensitive position, suitability or fitness for Federal employment, fitness for contract employment, or eligibility for physical and logical access to federally controlled facilities or information systems."[151] At the time, the process was managed by OPM, but as Chapter 1 indicated, their failures resulted in the creation of NBIB, which combines efforts with the Defense Counterintelligence and Security Agency. It is much more likely dishonesty regarding school attendance and completion would be caught under the new process.

Snowden also lied about being a "senior advisor" at the CIA on his resume to the NSA. It was later revealed that he was an entry level computer technician who embellished his roles and responsibilities to create a façade of competence and prestige.[152] Had Snowden lied about that on

[151] United States Office of Personnel Management. Completing your Investigation Request. (2018)
[152] Mark Hosenball. Reuters, U.S. House Panel Slams Former NSA Contractor Snowden. (2016)

an SF-86, it would have likely been discovered, but open source research does not indicate that he did. The seam between what is reported on an applicant's SF-86 and resume presents another opportunity for background investigators to identify discrepancies, especially after researching the applicant's actual role with the former employers. For credibility to be established, all three checks should report the same information; what the employer says the applicant did for them should match what the SF-86 and resumes each claim.

The NSA has an office of Security and Counterintelligence. There is little open source information on the security office, but job postings indicate they investigate security matters within NSA. Given their assumed responsibilities, had Snowden's coworker reported him for the hooded sweatshirt he often wore containing inferences of classified information, it is likely he would have been investigated by counterintelligence special agents from that office. An internal investigation like that could have identified other indicators of his future actions and may have prevented the breach by immediately thwarting his access to classified information and preventing future privileges. This highlights the importance of symbiosis between security and intelligence personnel. The plethora of security incidents and his behavior at work should have brought his character into question many times. It is possible Snowden's case is an anomaly in the sense that he slipped through proverbial cracks in the system charged with identifying threats like him.

## Case Study: Risk Management Reform

Snowden's insider attack had a significant impact on national security across the globe. Although he has not yet been held accountable by the justice system for his crimes, attempts to mitigate similar risks in the future have been implemented. As chapter 2 discussed in great length, enterprise risk management became a significant consideration throughout the federal government between 2013 – 2016 when the ISC published an interagency standard for risk management to be used at federal facilities. Following Snowden's attack, the NSA answered the need for improved risk management by creating a senior executive chief risk officer position. In early 2014, Anne Neuberger was appointed to that position to help stem the tide of mounting privacy and civil rights issues following the breach.[153,154]

Prior to Snowden's breach, much less was known about the NSA or its activities. Even government officials joked that its acronym stood for "No Such Agency" instead of its true name because of the secrecy it inspired.[155] However, Ms. Neuberger's approach to the crisis involved increasing transparency as a means to inspire added trust in the NSA instead of the secrecy and suspicion it once used to protect its methods; "This is a little bit of a different approach for us from the traditional No Such Agency approach," Neuberger stated.[156] She further articulated her transparent methodology comparing the NSA to a "black box" and explaining that Americans are curious to know what is contained within.[157] Therefore, Neuberger's approach blends transparency to garner the public's trust with risk-informed policies that determine when an activity is worth it.

Neuberger began her enterprise risk management (ERM) reform by first engaging key leaders and stakeholders throughout the NSA. As chapter 2 explained, having leadership approval across any organization is essential for ERM to be effective at establishing correct context, which is step 1 in GSA's *Playbook: Enterprise Risk Management for the US Federal*

[153] LinkedIn, Anne Neuberger. (2020)

[154] Larry Downing. Wall Street Journal, NSA Forms Cybersecurity Directorate Under More Assertive U.S. Effort. (2019)

[155] Jason Pontin. Aspen Ideas, No Such Agency: The NSA Explained. (2018)

[156] Alyza Sebenius. Insurance Journal, Behind the Foggy Curtain. (2019)

[157] Ibid.

*Government*. Additionally, incorporating leadership from the onset enabled Neuberger to determine the NSA's risk appetite and blend in step 2, identifying the actual risks.[158,159] Neuberger described the importance of defining NSA's risk appetite as "critical," and further developed a set of accompanying risk principles.[160]

NSA's initial approach at implementing ERM did not stop with engaging senior NSA leaders. Neuberger led 11 working groups of between 10 and 20 employees each that focused on security events, like Snowden. The exact topics of each working group meeting are not revealed in open source reporting, but they built the NSA's risk model carefully analyzing each event; using traditional investigative questions like what went wrong, what drove it, and the severity of the event. Incorporating hundreds of employees into the development of the framework created employee-influencers who helped pilot the program from inception.[161] Additionally, as chapter 2 illustrated, the working groups aided communicating ERM's important to the future of NSA. To further open lines of communication about it, Neuberger spoke often at town hall meetings and other internal forms of social media, which fostered two-way discussion that was vital for the employees' understanding.[162]

The following steps of GSA's ERM playbook were accomplished through Neuberger's time in the CRO role. Many organizations focus their ERM framework internally, but she spoke to the fact that NSA went to great lengths at analyzing the broader picture, to include how intelligence operations could impact foreign relations.[163] An area that Neuberger did

[158] DHS. The Risk Management Process for Federal Facilities. (2016)
[159] Hillary Tuttle. RM Magazine, How the NSA's First CRO is Integrating Risk Management into National Security. (2015)
[160] Ibid.
[161] Ibid.
[162] Ibid.
[163] Ibid.

exceptionally well implementing ERM was understanding the balance of “traditional security risks” and the new ones created in the cyber domain. Her clear delineation between the two risk areas allowed her team to create reliable and repeatable processes that every employee can follow.[164] Making it easy and identifying the key areas of risk for NSA has made ERM part of the “way we do business,” said Neuberger.

It is unknown based on unclassified information if the risk Snowden posed was communicated, not only throughout the NSA, but between all the agencies and companies he worked for. Although, since he was able to keep getting jobs and the subsequent access, it is unlikely he was ever labeled a priority risk, if it was communicated at all. This highlights the need for improved information flow and prioritization because it would enable more countermeasures to be devoted to the mitigation, which in Snowden’s case could have saved lives and billions of dollars.

Given the destruction Snowden caused, it is difficult to imagine that good could come from his crimes. However, NSA invested heavily in ensuring a sound risk framework is in place that can prevent a similar crisis in the future. Neuberger even commented that NSA’s transparency in response to the breach is a very new and seemingly unusual departure from “the way NSA operated three or four years ago.”[165] This illustrates tremendous effort placed on the agency to step outside its comfort zone for effective mitigation. Given the increased transparency, it is also likely risk information flow has improved throughout the NSA and associated organizations.

[164] Anne Neuberger. Cyberscoop, NSA’s Anne Neuberger on What Enterprises Need to Weigh When It Comes to Cloud Security. (2019)
[165] Hillary Tuttle. RM Magazine, How the NSA’s First CRO is Integrating Risk Management into National Security. (2015)

# Chapter 3: Conclusion

In conclusion, national security is paramount to the American way of life, yet adversaries of the U.S. constantly seek to disrupt that liberty through sabotage, espionage, and extremist ideologies. Unfortunately, insider threat has become an increasingly prevalent tactic used by FIEs to meet that objective. Carnegie Mellon University describes insider threats as individuals who use their authorized access to harm the organization. Historically, malicious insiders have conducted violence, sabotage, theft, and espionage. However, there are many incidents of non-malicious insider threat incidents known as unintentional insiders. Poor training, negligence, and rushed schedules can all create unintentional insider events, which occur when the employee did not mean to create a breach.

The DoD has experienced many insider attacks that hurt national security, including both malicious and unintentional. In Afghanistan, Buckshot Yankee represents a historical breach that was likely perpetrated by an unintentional insider. The loss was significant because it compromised operational information and it is still unclear which FIE benefited from the breach. Edward Snowden's unauthorized disclosures of an unknown amount of classified information represents an extremely harmful malicious insider who conducted espionage and helped U.S. adversaries across the globe. Snowden's breach will lead to billions of U.S. dollars lost in technology development and the U.S.' intelligence capabilities.

To mitigate the impact insider threats have on national security, there are many federal mandates across all branches of the executive. Federal security programs that effectively adhere to the mandates and incorporate intelligence can provide more holistic and efficient protection. Additionally, security programs benefit from including risk management in their decision cycle as it helps create a risk informed culture. A stronger risk culture likely leads to a more risk adverse atmosphere that facilitates interagency coordination as some departments lack authorities to conduct investigations that could prevent some of the most damaging insider attacks. Nidal Hassan's attack at Ft. Hood perfectly illustrates this point because the FBI withheld information from the DoD that could have led to his arrest prior to the shooting. Unfortunately, DoD was not privy to Hassan's communication with a known terrorist ideologue due to their authorities preventing them from collecting on U.S. persons and national security felt the sting of 32 lost lives as a result.

## Thesis Conclusion

This thesis articulates how federal security programs can better safeguard national security from insider threats when integrating intelligence and risk management. In some cases, security alone may suffice, but security programs that use intelligence analysis and risk management are positioned to better protect their organization by allocating resources commensurate to the threat landscape. The seamless integration of the disciplines also causes the program to be more cost effective and easier to scale due to the increased focus and improved efficacy. However, it was discovered that integrating the disciplines also requires improved integration across executive departments, such as DoJ, DoD, and DHS, based on each department's unique authorities and mission focus. Cohesion between departments has historically been a challenge, but could be overcome by a presidential directive and increased joint working groups on initiatives that involve multilateral equities.

Chapter one introduced the importance of integrating the various disciplines of intelligence with security programs. For security programs to be useful, they must know their threat landscape and intelligence analysis is required to gain that complete understanding. Opensource intelligence (OSINT) collection and analysis is used, but adversaries do not often post their malicious intent on social media, making it difficult to find it using OSINT alone. Geospatial intelligence is also used, which enables organizations to visually depict their operating environment using commercial resources such as Google Maps. Yet, the information is often outdated and fails to capture the future intent of adversaries. Instead, counterintelligence emerged as the most prevalent intelligence discipline given its internal focus and protection objectives, making it the most likely to reduce the possibility of a security incident.

Counterintelligence is a discipline of intelligence meant to disrupt adversarial actions against the U.S., to include espionage, sabotage, subversion, and terrorist attacks. A venue for counterintelligence is the National Insider Threat Task Force (NITTF), which enables organizations to become more proactive in their defense against insider threats. The NITTF significantly reduces bureaucracy and provides invaluable resources that empowers security programs throughout federal workplaces and especially the DoD. The creation of the NITTF was a result of EO 15587 and built around counterintelligence principles that defend national security. Yet, the NITTF's efforts could still be scaled for greater impact on insider threat detection and prevention at organizations with access to classified information across the country. The NITTF offers a great service by leading the effort to standardize insider threat programs by publishing helpful framework material, but a more hands-on, consultative approach would likely yield better security results.

It was discovered that previous executive administrations also recognized the necessity to use intelligence for better protection and national security. The Executive Orders 10450, 12333 and 12968 all facilitated/required the integration of intelligence for the sake of better security in one form or another. Executive Order 10450 mandated that federal employees must complete background investigations as a requirement of employment. This set the stage for counterintelligence to be more involved in the hiring process, which likely eliminated countless potential employees that would have been security risks, such as insider threats. Executive Order 12333 granted special collection authorities that extended the power of counterintelligence special agents and their agencies they work for. And Executive Order 12968 outlined policies that allowed federal employees access to classified information, but stipulated the conditions of governance that security facilitated.

It was no coincidence that the DoJ's FBI was assigned primacy for all counterintelligence matters, meaning other departments also have investigative capacity, but the FBI can take lead if operational interest is established. The FBI's lead role in counterintelligence investigations is complimented by their significant contribution in the *Domestic Approach to National Intelligence*, as written by James Clapper, the former Director of National Intelligence. The goal of protecting national security is complicated by the need to also protect privacy, civil liberties, and civil rights; making the collection on U.S. persons a crime unless the appropriate authorities are granted. However, the DHS is responsible for the unified national effort to secure the U.S. by preventing and deterring terror attacks and responding to other threats and hazards, as the *Domestic Approach to National Intelligence* makes clear.[166] The DoD's collection authorities focus on foreign targets, making domestic collection for their security purposes a joint effort between the FBI and DHS, and often a result of their criminal investigations.

[166] https://www.dni.gov/files/documents/Newsroom/DomesticApproachtoNationalIntelligence

Further study should take a deeper dive into DoD Manual 5240.01, which governs the conduct of collection activities for organizations throughout the government. While this thesis was being drafted, the appeals court ruled that some of the programs Snowden illicitly released to the public were illegal. So, an in-depth analysis of DoD Manual 5240.01 may provide additional considerations for domestic collection for national security as it was discussed in chapter three, but it is unlikely much more would have been gleaned as it pertains directly to security programs.

Furthermore, studying how organizations can build resilience within their security program may be an important consideration for follow on research. Resilience directly impacts security as it highlights how an organization can overcome security events that were not prepared for in advance, either with stronger countermeasures or an adjustment to controls already in place. The higher an organization's resilience, the more likely it is to defend itself against a range of threats that cannot be specified in advance by being able to adapt to the threat landscape more quickly.

This study examined how it could be advantageous for intelligence to be integrated into federal security programs, but was unsure how that relationship and implementation would be managed. The DoD Manual 5240.01 was very important as it clearly outlined the restrictions placed on the organizations in question and highlighted specific circumstances of how collection on U.S. persons is to be conducted and by whom. Additionally, it was determined that there are no national level intelligence assets allocated to federal security programs that collect domestically, making threat intelligence primarily a counterintelligence (CI) function or law enforcement activity for the DOJ or DHS, even for the DoD.

Chapter two demonstrated the strategic benefits of using risk management to complement security programs, as well as how it can influence ongoing security practices. Like intelligence integration, there are federal mandates that require risk management be an integral part of federal organizations. However, the intent of many of them is to influence fiscally responsible decision making, much more than improve security programs. Additionally, risk management is largely a function of DHS, as they are responsible for the protection of federal buildings. However, the correct use of risk management would aid an organization's leadership determine the most appropriate balance between security and risk tolerance, which must be prioritized and communicated constantly.

Risk management plays into a holistic security model as the identification and analysis portions of the risk cycle (steps 2 and 3) are instrumental for illuminating the threat landscape. Without understanding the true nature of specific threats, security programs are unable to effectively allocate resources. Additionally, in concert with the value intelligence adds through red team operations and OSINT, risk analysis can mitigate the identified vulnerabilities that create the most risk. When fiscally-minded decision making matters most, allocating financial resources to what makes the greatest impact could be the difference between life or death, and/or leaders who achieve their objectives with limited budgets.

As the NSA learned from the Snowden leaks, risk management is a continuous process that does not end once an individual risk is mitigated. Instead, organizations adapt and learn from risk events to prevent future ones. As Anne Neuberger implemented in the NSA, it takes an enterprise wide approach that begins with senior leadership's buy in. Communication and prioritization are also imperative and must not get lost in organizational silos. Instead, risk appetite statements should be accessible to employees, as the DHS suggests in their implementation guidelines, and employees need to feel like their voices are heard. To capture this effectively, Ms. Neuberger used working groups to include employees at many levels to instill the benefit of them all working together toward their mutual goal – risk mitigation via implementation of the risk management process.

The DHS's ISC and GSA published a plethora of risk management guidance and material pertaining to federal usage and implementation. However, few sources were found that indicate risk management has become an integral aspect of security management. Even with Ms. Neuberger's applaudable efforts at NSA, it is unclear how much their federal police force makes risk management a conscious consideration in their daily activities. Unfortunately, the effectiveness of risk management is limited to the employment layers that use it; meaning any organization that commits to creating a risk informed culture will benefit when employees at every level make smarter, more risk conscious decisions. To enable this, Circular A-123 makes the point that organizations should focus on prioritization as a key process in risk management. Since no organization can identify every risk, they are incapable of stopping every incident, making it imperative to focus on major risks rather the myriad of smaller ones. Intelligence is used to constantly discover emerging threats and evaluate the potential impact of existing ones, which help inform the priority level and associated response.

Chapter three discusses the various types of insider threats and illustrates how they can impact national security. Insider threats are complex because they can be malicious or unintentional, but each kind creates internal vulnerabilities as a result of their authorized access to classified information, employees, or assets. In some cases, such as Nidal Hasan, their access is used for murder, motivated by extreme religious ideologies. Other insiders, like Snowden, use their access for espionage, which impacts national security because of the strategic advantage their breaches offer U.S. adversaries.

The term ‘national security’ can mean something different based on varying perspectives. Furthermore, the research for this study determined national security implies freedom from foreign dictation, economic and political stability, and unchallenged sovereignty. As the power gap between the U.S. and its near peer adversaries rapidly outpaces most every other nation, the competition for even the smallest advantage rages on. Insiders play an integral role in that effort as they offer pieces of information that create a broader, more accurate sense of U.S. objectives at the strategic, operational, and tactical levels.

The advancements in the cyber domain make the exfiltration of data easier than ever, as well as the contact, recruitment, and handling of sources. The ongoing conflict in the cyber domain additionally creates an opportunity for foreign adversaries to sow civil discord and influence internal politics, such as elections. It also makes attacks and insider activity more difficult to discover and, consequently, defend against. While on a DoD network, users consent to monitoring, yet successful mitigation of malicious activity is difficult because the system administrators who are observing are not always savvy enough to discern between malign and legitimate usage. This strengthens the need for them to be tied into counterintelligence personnel, who are more likely to identify indicators of compromise or insider danger that benefits an adversary.

While the specific consequences of insider threats may vary case by case, most have considerable implications on national security. Snowden’s illicit disclosures gave adversaries, and allies alike, a means of challenging and defying U.S. sovereignty. In effort to recapture what was lost, the U.S. intelligence community and political operatives must navigate an international relations environment complicated by a sense of betrayal and the resulting loss of trust. Additionally, U.S. Armed Forces were placed in elevated danger as a result of their opposing combatants gaining a better understanding of their plans, weapons, and how to defeat them on the battlefield. It is also increasingly difficult to project a sense of power on the global stage when threats from within the ranks cause some of the greatest damage; this weakens the U.S.' political standing and makes it more likely a near peer adversary will engage in conflict.

The very act of a foreign adversary recruiting, or exploiting, an employee of the U.S. government, to divulge classified information for their gain is an aggressive attack against sovereignty, which destabilizes peace. For this reason, insider threat programs should be built up in effort to establish a more proactive defense against such actions. No risk appetite statement statements could be found in the open web, but a strictly low acceptance for insiders should be included in each DoD organization's as a result of the potential for compounding impacts. If insider risk is considered, the risk can be mitigated using the suggestions mentioned throughout this study; doing so is likely to reduce the constant degradation of U.S. power and interest, both internally and abroad, and will therefore improve national security.

There is also little open source information that shows other DoD agencies went through as much effort implementing risk management as NSA, which may represent a potential vulnerability. However, the fact that NSA's efforts are publicized could simply be a result of the NSA's need to recapture public trust, while other agencies may guard their risk management activity more closely because there is no need to share it. Regardless, it is likely that DoD could improve dramatically with their efforts to apply risk management to their security programs. Even though DHS has responsibility within government, every DoD security program can implement a basic risk management process that will improve their protection.

Aside from security specific personnel, many DoD organizations, to include military units, have anti-terrorism and force protection officers (ATFP) to augment general security. Given their duties, they are likely a strong audience to begin instilling risk-informed decision making. These individuals are often tasked with broadcasting threats in their local environments, so adding the extra layers of analysis (vulnerability and impact) necessary to provide a risk score would certainly garner more attention from the employees due to it then becoming personal. Additionally, the ATFP officers could become more versed in NITTF's publications to improve the integration of insider threat programs throughout DoD. This approach offers multiple layers of risk integration and combines it with countering insider threat, which increases their effectiveness and potential to further safeguard national security.

To protect national security from emerging threats with the highest efficacy, it is suggested that stronger cohesion is mandated between departments through increased interagency efforts. Currently, there are stigmas attached to certain federal organizations, which are never challenged when everyone works in a silo. Yet, the negativity must be eliminated since everyone's objective is largely the same – protect the U.S. and its interests. Eliminating the stigmas and departmental competitions is most likely to happen through more efforts such as the Joint Terrorism Task Forces (JTTFs) and NITTF. The JTTFs are comprised of special agents from many departments, who work together to counter terrorism. Increasing the amount of interagency efforts would not only foster better personal relationships, but allow each organization to share resources and authorities. Doing so would likely equate to more well-rounded teams and shared equities, which would increase the amount of tipping and queuing of operational details between departments that could potentially prevent an attack.

Employees within the DoD have Annual training requirements. Some are computer based and others require in-person briefings. An increase of insider threat training for all employees is recommended to increase the reporting of indicators. As this study illustrated with Snowden and his provocative sweatshirt, even the smallest indicators of compromise matter because they may help with identifying a threat. The suggested changes to the annual insider threat training include more emphasis on potential indicators and the reporting procedures. With that, employees need to feel safe about reporting their coworkers for events that are not blatantly an indication of espionage or another form of wrong doing. Clearly articulating how the reporting employees will remain anonymous and be afforded protection from retribution will likely place them at ease. Additionally, the training must illustrate how it is everyone's duty to report for the sake of national security; doing so makes them a hero – not a 'snitch,' which is another stigma that must be overcome in the training.

Another way to bolster national security through annual training is to create and implement risk management and threat analysis training for security personnel. This would ensure that the personnel responsible for the organization's security, not just the management, are well versed in the risk management process. Additionally, it would make them adept at identifying and analyzing threats that they may have previously not had the wherewithal to consider. Making in annual requirement instead of a one-time training is suggested because it would refresh and hone the recipients' skills.

The final suggestion for this thesis is a considerable increase to the DoD budget, or a reallocation of funds, to train and hire holistic security personnel meant to carry out the lessons learned in this study. It is recommended that each DoD organization add two holistic security officers, ranks GS 14-15, to their risk management department, purely to integrate the various disciplines of security along with risk management and intelligence. Their jobs would not be to perform security activities, but more so review and advise on the organization's security policies. Then they would perform audits to ensure the policies are being executed to the prescribed standard, or adjustments would be made.

These professionals would be well trained and versed in both physical and cyber security, and they would be charged with the elimination of the silos each discipline likely operates in. They would also ensure the policies are written in a manner where intelligence is shared between the departments and used for risk analysis. This suggestion would be immensely beneficial at ensuring the various lessons learned from this study are used in a manner that would create better security programs. Additionally, it would ensure each DoD organization is making risk management a deliberate consideration for their security programs, which has the potential to save money while offering better protection.

It is understood that many of the aforementioned suggestions and lessons learned throughout this study would require a considerable amount of organizational change across many departments. However, the time and concerted effort invested would result in more harmonious synchronization between executive departments and equate to improved national security. This could be initiated by a presidential directive and managed by the ISC. A future study could apply organizational change theory to assess exactly what areas would need to change for each department and potentially generate a change management strategy.

In conclusion, this thesis illustrates the necessity to integrate intelligence and risk management practices into federal security programs to protect national security. The integration of each ancillary discipline allows for a stronger balance between security and risks, along with a more effective allocation of resources. It also enables organizations to identify whatever threats are on the horizon and meet them with decisive ad deliberate action, as opposed to hoping a generic security program will protect against them when they occur. Additionally, insider threats are rising in prevalence and pose a significant risk to national security. The adherence to stronger integration will enable organizations to defend against them with urgency and prevent additional losses, which could be in the form of American lives, international relations, or peace.

***THIS PAGE INTENTIONALLY LEFT BLANK***

# Bibliography

A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen. (2003, August 14). Retrieved from https://oig.justice.gov/special/0308/index.htm

About the NRO. (n.d.). Retrieved from https://www.nro.gov/About-NRO/

After Action Report: Washington Navy Yard, After Action Report: Washington Navy Yard § (2014). https://www.policefoundation.org/wp-content/uploads/2015/05/Washington-Navy-Yard-After-Action-Report.pdf.

"APA PsycNet." American Psychological Association. Accessed November 21, 2020. https://psycnet.apa.org/record/2006-03272-025.

All About Security Clearances. (n.d.). Retrieved from https://www.state.gov/m/ds/clearances/c10978.htm

An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence. (1994, November 01). Retrieved from https://fas.org/irp/congress/1994_rpt/ssci_ames.htm

Ana Montes: Cuban Spy. (2016, July 20). Retrieved from https://www.fbi.gov/history/famous-cases/ana-montes-cuba-spy

Armstrong, T. (2017, November 07). Do You Know Which Cybersecurity Tools Really Address Insider Threat? Retrieved from https://www.observeit.com/blog/do-you-know-which-cybersecurity-tools-really-address-insider-threat/

Blackburn, Robert. “Enterprise Risk Management (ERM) versus Traditional Risk Management Best Practice.” blackburn group inc. Accessed May 5, 2020.

https://www.blackburngroup.com/newsroom/enterprise-risk-management-erm-versus-traditional-risk-management-best-practice.

Bradshaw, T. (n.d.). IP Address Cards. Retrieved from https://support.recordedfuture.com/hc/en-us/articles/115001398968-IP-Address-Cards

Brown, D. (2013, March 22). 10 Things You Might Not Know about the National Geospatial-Intelligence Agency. Retrieved from https://news.clearancejobs.com/2013/03/22/10-things-you-might-not-know-about-the-national-geospatial-intelligence-agency/

Burmester, Mike, Emmanouil Magkos, and Vassilis Chrissikopoulos. Florida State University , n.d. http://www.cs.fsu.edu/~burmeste/333.pdf.

Cameron, E. S. (2015, December 01). Proof That Positive Work Cultures Are More Productive. Retrieved from https://hbr.org/2015/12/proof-that-positive-work-cultures-are-more-productive

Carfagno, D. (2018, December 31). What is a Security Operations Center & Why Is It Important? Retrieved from https://www.blackstratus.com/what-is-a-security-operations-center-and-why-is-it-important/

Carney, John. “Cisco.” Cisco, 2011. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/pl-security.pdf.

Central Intelligence Agency Library. (2008, June 28). Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_1.htm

Cherdantseva, Yulia, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and

Kristan Stoddart. “A Review of Cyber Security Risk Assessment Methods for SCADA Systems.” Computers & Security. Elsevier Advanced Technology, October 13, 2015. https://www.sciencedirect.com/science/article/pii/S0167404815001388.

Chief Financial Officers Council , 2016. https://cfo.gov//wp-content/uploads/2016/07/FINAL-ERM-Playbook.pdf.

Clark, Charles S. “Agencies Get a New Playbook for Managing Risks.” Government Executive, June 12, 2019. https://www.govexec.com/management/2016/08/agencies-get-new-playbook-managing-risks/130459/.

Clement, J. “U.S. Government Cyber Security Incidents 2018.” Statista, January 17, 2020. https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/.

Clinton, William. Executive Order 12977 § (1995).

Cole, M., & Esposito, R. (2013, August 23). How Snowden did it. Retrieved from https://www.nbcnews.com/news/world/how-snowden-did-it-flna8C11003160

Costa, Daniel. "CERT Definition of 'Insider Threat' - Updated." CERT Definition of 'Insider Threat' - Updated. March 07, 2017. Accessed November 21, 2020. https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html.

“Cyber-Physical Attacks Are Growing alongside the IoT: Synopsys.” Software Integrity Blog, October 8, 2019. https://www.synopsys.com/blogs/software-security/cyber-physical-attacks/.

Damron. “Login.” May 2004 - Volume 422 - Issue: Clinical Orthopaedics and Related

Research®. Accessed May 5, 2020. https://journals.lww.com/clinorthop/Fulltext/2004/05000/Mass_Casualties_in_the_Oklahoma_City_Bombing.

Deppisch, Breanne. "DHS Was Finally Getting Serious About Cybersecurity. Then Came Trump." POLITICO. Accessed May 5, 2020. https://www.politico.com/news/magazine/2019/12/18/america-cybersecurity-homeland-security-trump-nielsen-070149.

"Executive Services Directorate." DoD Issuances. Accessed May 5, 2020. https://www.esd.whs.mil/Directives/issuances/dodi/.

"Executive Orders." National Archives and Records Administration. Accessed November 21, 2020. https://www.archives.gov/federal-register/codification/executive-order/12356.html#1.1.

"Facility Protection: Implications of the Navy Yard Shooting on Homeland Security." - FACILITY PROTECTION: IMPLICATIONS OF THE NAVY YARD SHOOTING ON HOMELAND SECURITY. Accessed May 5, 2020. https://www.govinfo.gov/content/pkg/CHRG-113hhrg87184/html/CHRG-113hhrg87184.htm.

Farivar, C. (2016, October 20). Feds seized 50TB of data from NSA contractor suspected of theft. Retrieved from https://arstechnica.com/tech-policy/2016/10/feds-nsa-contractor-stole-at-least-50tb-worth-of-highly-classified-data/

Fonseca, Maggie, Josh Epstein, and Sai Chavali. "The Primary Factors Motivating Insider

Threats." ObserveIT. June 19, 2020. Accessed November 21, 2020. https://www.observeit.com/blog/primary-factors-motivating-insider-threats/.

Gaskell, Stephanie. "Snowden Lasted 5 Months in Army." POLITICO. June 10, 2013. Accessed November 21, 2020. https://www.politico.com/story/2013/06/edward-snowden-army-discharge-092486.

*General Security Risk Assessment*. Alexandria, VA: ASIS International, 2003.

Graff, Garrett M. "China's Five Steps for Recruiting Spies in the US." Wired. Accessed November 21, 2020. https://www.wired.com/story/china-spy-recruitment-us/.

Gray, Kevin. “Family of Victim in Navy Yard Shooting Sues U.S. for Negligence.” Reuters. Thomson Reuters, November 8, 2013. https://www.reuters.com/article/us-usa-shooting-lawsuit/family-of-victim-in-navy-yard-shooting-sues-u-s-for-negligence-idUSBRE9A70YH20131108.

“GSA Launches Enterprise Risk Management Playbook.” GSA, November 1, 2018. https://www.gsa.gov/about-us/newsroom/news-releases/gsa-launches-enterprise-risk-management-playbook.

Gumbel, A. (2015, April 13). Oklahoma City bombing: 20 years later, key questions remain unanswered. Retrieved from https://www.theguardian.com/us-news/2015/apr/13/oklahoma-city-bombing-20-years-later-key-questions-remain-unanswered

Hamburg, Ileana, and Kira Rosa Grosch. “Aligning a Cybersecurity Strategy with Communication Management in Organizations.” IntechOpen. IntechOpen, September

19, 2018. https://www.intechopen.com/books/digital-communication-management/aligning-a-cybersecurity-strategy-with-communication-management-in-organizations.

Harrell, Brian. Department of Homeland Security, April 17, 2020.

Henderson, William. “Aaron Alexis and the Failure of the Federal Security Clearance Process.” ClearanceJobs, December 18, 2018. https://news.clearancejobs.com/2013/10/10/aaron-alexis-failure-federal-security-clearance-process/.

“Homepage: CISA.” Cybersecurity and Infrastructure Security Agency CISA. Accessed May 5, 2020. https://www.cisa.gov/.

Holpuch, Amanda. "Journalists Who Broke NSA Story in Guardian Dedicate Award to Snowden." The Guardian. April 11, 2014. Accessed November 21, 2020. https://www.theguardian.com/world/2014/apr/11/journalists-nsa-guardian-polk-award-snowden.

Hosenball, Mark. "U.S. House Panel Slams Former NSA Contractor Snowden." Reuters. September 15, 2016. Accessed November 21, 2020. https://www.reuters.com/article/us-usa-security-snowden/u-s-house-panel-slams-former-nsa-contractor-snowden-idUSKCN11L2PU.

Ilascu, Ionut. “FBI: Hackers Sending Malicious USB Drives & Teddy Bears via USPS.” BleepingComputer. BleepingComputer.com, March 30, 2020. https://www.bleepingcomputer.com/news/security/fbi-hackers-sending-malicious-usb-drives-and-teddy-bears-via-usps/.

INTelligence: Human Intelligence. (2010, October 21). Retrieved from https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html

"Insider Threat - Workplace Violence." Cybersecurity and Infrastructure Security Agency CISA. Accessed November 21, 2020. https://www.cisa.gov/workplace-violence.

“ISC Risk Management Process.” GSA, January 8, 2018. https://www.gsa.gov/real-estate/design-construction/engineering-and-architecture/security-engineering/isc-risk-management-process.

Kopan, Tal. "10 Things to Know about Snowden." POLITICO. June 10, 2013. Accessed November 21, 2020. https://www.politico.com/story/2013/06/10-things-to-know-about-edward-snowden-092491.

Jones, K. (n.d.). Implementing Insider Threat Programs. DSS Access, 5(4). doi:https://www.dss.mil/Portals/69/documents/about/err/DSS_ACCESS_v5i4_web.pdf

“Lack of Senior Manager Support Impairs Risk Management.” ERM. North Carolina State University, May 1, 2012. https://erm.ncsu.edu/library/article/lack-of-senior-manager-support-impairs-risk-management.

Lessons from Fort Hood: improving our ability to connect the dots, Lessons from Fort Hood: improving our ability to connect the dots § (2012).

Lord, N. (2019, April 26). What is a Security Operations Center (SOC)? Retrieved from https://digitalguardian.com/blog/what-security-operations-center-soc

Loyear, Rachelle. “How Do You Communicate Security Risk to Business Executives?” Risk and

Resilience Hub, April 12, 2019. https://www.riskandresiliencehub.com/how-do-you-communicate-security-risk-to-business-executives/.

Management Accountability and Control, Circular No. A-123 § (1995).

McVeigh, Karen, and Paul Lewis. "Aaron Alexis Passed Recent Background Checks by Employer and Gun Store." The Guardian. Guardian News and Media, September 17, 2013. https://www.theguardian.com/world/2013/sep/17/aaron-alexis-background-check-employer-gun.

Meek, James, Et al. ABC News, Intel Heads: Edward Snowden Did 'Profound Damage' to U.S. Security. (2014)

National Network of Fusion Centers Fact Sheet. (2018, December 17). Retrieved from https://www.dhs.gov/national-network-fusion-centers-fact-sheet

National Security Agency. (n.d.). Retrieved from https://www.nsa.gov/What-We-Do/

"No Such Agency: The NSA Explained: Aspen Ideas." Aspen Ideas Festival. Accessed November 21, 2020. https://www.aspenideas.org/sessions/no-such-agency-the-nsa-explained.

Pakistani man executed for CIA killings. (2002, November 02). Retrieved from http://edition.cnn.com/2002/LAW/11/14/cia.killings.execution/index.html

Robinson, J. (2001, November 15). Internal Threat - Risks and Countermeasures. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/internal-threat-risks-countermeasures-475

Reagan, Ronald. Executive Order 12333 § (1981).

Reese, Shawn. “Congressional Research Service.” Congressional Research Service. Accessed March 6, 2017. https://fas.org/sgp/crs/homesec/R43570.pdf.

Reflecting on the Ability of Enterprise Security Policy to Address Accidental Insider Threat - IEEE Conference Publication. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6978924.

Riechmann, Deb. "Costs of Snowden Leak Still Mounting 5 Years Later." AP NEWS. June 04, 2018. Accessed November 21, 2020. https://apnews.com/article/797f390ee28b4bfbb0e1b13cfedf0593.

Report to the Committee on Oversight and Government Reform, House of Representatives, Report to the Committee on Oversight and Government Reform, House of Representatives § (2016).

Risk Management Fundamentals, Department of Homeland Security. Homeland Security Risk Management Doctrine § (2011).

Rittenberg, Larry, and Frank Martens. “COSO.” COSO. Committee of Sponsoring Organizations of the Treadway Commission, 2012. https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf.

Savage, Charlie. "House Intelligence Committee Urges No Pardon for Edward Snowden." The New York Times. September 16, 2016. Accessed November 21, 2020. https://www.nytimes.com/2016/09/16/us/politics/edward-snowden-no-pardon-house-intelligence.html.

Sebenius, Alyza, and Name *. "Behind the Foggy Curtain: A Peek Into Secret U.S.

Cybersecurity Operation." Insurance Journal. October 15, 2019. Accessed November 21, 2020. https://www.insurancejournal.com/news/national/2019/10/15/545486.htm.

Snedaker, Susan, and Chris Rima. “Risk Acceptance.” Risk Acceptance - an overview | ScienceDirect Topics. Accessed May 5, 2020. https://www.sciencedirect.com/topics/computer-science/risk-acceptance.

"Snowden Wore EFF Hoodie and Kept a Copy of the Constitution at His Desk." The Daily Dot. March 02, 2020. Accessed November 21, 2020. https://www.dailydot.com/unclick/snowden-eff-hoodie/.

Stering, Robert. *Police Officers Handbook: an Introductory Guide*. Sudbury: Jones and Bartlett, 2005.

Soto, Alonso, and Brian Winter. "Saab Wins Brazil Jet Deal after NSA Spying Sours Boeing Bid." Reuters. December 18, 2013. Accessed November 21, 2020. https://www.reuters.com/article/us-brazil-jets/saab-wins-brazil-jet-deal-after-nsa-spying-sours-boeing-bid-idUSBRE9BH11C20131218.

Stilwell, Blake. "The Worst Cyber Attack in DoD History Came from a USB Drive Found in a Parking Lot." We Are The Mighty. October 30, 2020. Accessed November 21, 2020. https://www.wearethemighty.com/history/worst-cyber-attack-usb?rebelltitem=1#rebelltitem1.

Stone, Jeff. "NSA's Anne Neuberger on What Enterprises Need to Weigh When It Comes to Cloud Security." CyberScoop. November 06, 2019. Accessed November 21, 2020. https://www.cyberscoop.com/video/anne-neuberger-nsa-cloud-security-cybertalks-2019/.

"Swiss President Would Back Criminal Probe against NSA Leaker." Reuters. June 16, 2013. Accessed November 21, 2020. https://www.reuters.com/article/us-usa-security-switzerland-snowden/swiss-president-would-back-criminal-probe-against-nsa-leaker-idUSBRE95F09120130616.

The District of Columbia Communications Interoperability Summit:A 6 Year Review of the Washington Navy Yard Shooting, The District of Columbia Communications Interoperability Summit:A 6 Year Review of the Washington Navy Yard Shooting § (n.d.).

"The Federal Protective Service." Department of Homeland Security, January 13, 2020. https://www.dhs.gov/topic/federal-protective-service.

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard § (2016).

Tuttle, Hilary, Andy Niver, Tom Williams, and Joshua Gold. "Home." Risk Management. April 21, 2016. Accessed November 21, 2020. http://www.rmmagazine.com/2015/12/01/mission-critical-how-the-nsas-first-cro-is-integrating-risk-management-into-national-security/.

United States, Department of Defense. (2014). Joint Publication 2-01.3 Joint Intelligence Preparation of the Operational Environment.

United States, Department of Justice, Federal Bureau of Investigations. (2018). Criminal Justice Information Services Security Policy(Version 5.7).

Department of Justice Order Cyber Security Program, 0904 (2016).

"University of Maryland Won't Say If NSA Operates Secret Facility on Campus." Campus Reform the #1 Source for College News. Accessed November 21, 2020. https://www.campusreform.org/?ID=4789.

United States, Interagency Security Committee. (2015). Facility Security Plan. Sarve.

United States, National Insider Threat Task Force. (2017). Insider Threat Guide.

United States, National Insider Threat Task Force. (2018). Insider Threat Program Maturity Framework.

United States, Interagency Security Committee. (2013). The Risk Management Process for Federal Facilities.

Volz, Dustin. "NSA Forms Cybersecurity Directorate Under More Assertive U.S. Effort." The Wall Street Journal. July 23, 2019. Accessed November 21, 2020. https://www.wsj.com/articles/nsa-forms-cybersecurity-directorate-under-more-assertive-u-s-effort-11563876005.

*Vulnerability assessment of federal facilities*, U.S. Department of Justice, U.S Marshals Service § (1995).

Winter, Brian. "Exclusive: Brazil's Rousseff Wants U.S. Apology for NSA Spying." Reuters. September 04, 2013. Accessed November 21, 2020. https://www.reuters.com/article/us-usa-security-snowden-brazil/exclusive-brazils-rousseff-wants-u-s-apology-for-nsa-spying-idUSBRE98314N20130904.

Whittaker, Z. (2019, April 13). Hackers publish personal data on thousands of US police officers and federal agents – TechCrunch. Retrieved from

“Worm That Wreaked Havoc for US Military Likely a Progenitor of Red October.” Infosecurity

Magazine, March 12, 2014. https://www.infosecurity-magazine.com/news/worm-that-wreaked-havoc-for-us-military-likely-a/.

# Biographical Statement of Author

George Hyek is a native of Pittsburgh, PA, who currently resides in the national capital region. He earned his Bachelor of Arts in intelligence studies from Mercyhurst University. Since then, George has studied at the George Washington University and Joint Special Operations University, along with other federal training institutions/academies. George is currently a counterintelligence special agent for a defense agency and a U.S. Army Veteran. Throughout his professional experience, George served in joint special operations and the intelligence directorates of multiple strategic commands – making him an expert in interagency operations.