2017-12

Mitigating insider threats in the domestic aviation system: policy options for the Transportation Security Administration

Bean, Brian S.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MITIGATING INSIDER THREATS IN THE DOMESTIC AVIATION SYSTEM: POLICY OPTIONS FOR THE TRANSPORTATION SECURITY ADMINISTRATION

by

Brian S. Bean

December 2017

Thesis Co-Advisors: Lynda Peters
Erik Dahl

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE MITIGATING INSIDER THREATS IN THE DOMESTIC AVIATION SYSTEM: POLICY OPTIONS FOR THE TRANSPORTATION SECURITY ADMINISTRATION	**5. FUNDING NUMBERS**
6. AUTHOR(S) Brian S. Bean	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____n/a____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The Transportation Security Administration (TSA) defines insider threat as the risk posed by workers with inside access and knowledge to exploit vulnerabilities in the nation's transportation systems. In recent years, insiders have been leveraged by criminal and terrorist organizations to further nefarious plots in the aviation system. This thesis examines policy options for TSA to mitigate insider threats in the domestic aviation system and discusses the effectiveness of TSA's insider threat programs. This thesis also explores whether TSA can be more effective at insider threat prevention with additional intelligence collection authorities. The insider threat programs of the Department of Homeland Security's Office of Intelligence and Analysis, the Federal Bureau of Investigation, the United Kingdom's MI5, and federal defense contractor Lockheed Martin are analyzed to identify alternative solutions. At their core, insider threat policies center around three primary areas: security programs, counterintelligence programs, and organizational culture. TSA should establish its own counterintelligence program while continuing to fine-tune its security programs. Integrating counterintelligence and security programs enhances an organization's ability to detect and prevent insider threats. Finally, taking additional steps to establish a strong security ethos within the airport environment will help further "harden the target."

14. SUBJECT TERMS Transportation Security Administration (TSA), aviation, insider, access, insider threat, counterintelligence, Title 50, airport, Intelligence Community, vetting, credential, intelligence	**15. NUMBER OF PAGES** 103
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500 Standard form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

MITIGATING INSIDER THREATS IN THE DOMESTIC AVIATION SYSTEM: POLICY OPTIONS FOR THE TRANSPORTATION SECURITY ADMINISTRATION

Brian S. Bean
Field Intelligence Officer, Transportation Security Administration
BA, University of Utah, 2003
BA, University of Utah, 2003

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2017**

Approved by: Lynda Peters
Thesis Co-Advisor

Erik Dahl
Thesis Co-Advisor

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Transportation Security Administration (TSA) defines insider threat as the risk posed by workers with inside access and knowledge to exploit vulnerabilities in the nation's transportation systems. In recent years, insiders have been leveraged by criminal and terrorist organizations to further nefarious plots in the aviation system. This thesis examines policy options for TSA to mitigate insider threats in the domestic aviation system and discusses the effectiveness of TSA's insider threat programs. This thesis also explores whether TSA can be more effective at insider threat prevention with additional intelligence collection authorities. The insider threat programs of the Department of Homeland Security's Office of Intelligence and Analysis, the Federal Bureau of Investigation, the United Kingdom's MI5, and federal defense contractor Lockheed Martin are analyzed to identify alternative solutions. At their core, insider threat policies center around three primary areas: security programs, counterintelligence programs, and organizational culture. TSA should establish its own counterintelligence program while continuing to fine-tune its security programs. Integrating counterintelligence and security programs enhances an organization's ability to detect and prevent insider threats. Finally, taking additional steps to establish a strong security ethos within the airport environment will help further "harden the target."

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

ATSA	Aviation and Transportation Security Act of 2001
CI	counterintelligence
CPNI	Centre for the Protection of National Infrastructure
DHS	Department of Homeland Security
E.O.	executive order
FBI	Federal Bureau of Investigation
I&A	Department of Homeland Security Office of Intelligence and Analysis
IC	Intelligence Community
IE	Intelligence Enterprise
ISIS	Islamic State of Iraq and the Levant
ITDP	Insider Threat Detection Program
MI5	Military Intelligence Section 5
NCSC	National Counterintelligence and Security Center
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General
SIDA	Secure Identification Display Area
TSA	Transportation Security Administration
VIPR	Visible Intermodal Prevention and Response Program

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The Transportation Security Administration (TSA) defines insider threat as "one or more individuals with access and/or insider knowledge that allows them to exploit the vulnerabilities of the nation's transportation systems with the intent to cause harm."[1] Well-placed insider threats are ideally positioned within the nation's aviation system to further terrorist plots, carry out illegal smuggling operations, and conduct espionage. The literature demonstrates TSA operates several security programs designed to mitigate this threat, but these programs have some notable limitations. Recent terrorist plots within the national and international aviation systems have leveraged or attempted to leverage trusted insiders, thus highlighting the urgency of the issue for TSA.

TSA and the Federal Bureau of Investigation (FBI) agree insider threats represent one of aviation security's "most pressing concerns."[2] TSA employees alone account for over 50,000 aviation workers nationwide with access to sensitive areas and information at domestic airports. A 2017 House Homeland Security Committee report cites approximately 900,000 aviation workers at approximately 450 federalized airports.[3] Herein lies the potential insider threat within the aviation system from both TSA employees and other workers. Trusted insiders are familiar with weaknesses in internal policies and procedures, physical security, and information technology systems.[4] Many of these employees are granted secure identification display area (SIDA) badges, which give them physical access to many of the most sensitive areas of an airport, including planes on the runway and passenger baggage transiting areas.[5]

---

[1] Frank Deffer, *Transportation Security Administration Has Taken Steps to Address the Insider Threat but Challenges Remain* (Washington, DC: U.S. Department of Homeland Security, Office of the Inspector General, 2012), 2.

[2] Jennifer A Grover, *Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates* (Washington, DC: U.S. Government Accountability Office, 2016), 22.

[3] John Katko, *America's Airports: The Threat from Within* (Washington, DC: House Homeland Security Committee, 2017), 2.

[4] Deffer, *Transportation Security Administration*, 4.

[5] John Roth, *TSA Can Improve Aviation Worker Vetting* (OIG-15-98) (Washington, DC: U.S. Department of Homeland Security, Office of Inspector General, 2015), 8.

The severity of this threat to the domestic aviation system is significant and demonstrated by the following incidents. In 2013, avionics technician Terry Lee Loewen of Wichita, Kansas, attempted to detonate a vehicle-borne improvised explosive device outside the passenger terminal of Mid-Continent Airport from the secure (runway) side of the airport.[6] Another example is the 2009 case of Rajib Karim, who worked as an information technology employee with British Airways and was in regular contact with an overseas, al-Qaida terrorist leader of significant stature. Mr. Karim used his employee access to identify vulnerabilities and opportunities to attack the aviation system, including the recruitment of baggage handlers to place an explosive device onboard a U.S.-bound aircraft.[7] In 2014, Mark Quentin Henry, an employee of Delta Airlines, smuggled 153 firearms onto 17 different flights between Atlanta and New York City using his employee access to avoid scrutiny.[8] These cases illustrate serious vulnerabilities to insider threats within the aviation system.

This thesis reviews and analyzes the insider threat programs of four organizations in addition to TSA: the Department of Homeland Security's Office of Intelligence and Analysis (I&A), the FBI, the Centre for the Protection of National Infrastructure (CPNI, part of MI5 in the United Kingdom), and private company / federal defense contractor Lockheed Martin. Identifying the best practices from these organizations helps in analyzing the effectiveness of TSA's insider threat measures. This thesis also explores whether TSA can be more effective at insider threat prevention with additional intelligence collection authorities.

TSA currently mitigates insider threat issues through a variety of security measures and employee training initiatives.[9] These measures include the agency's Insider Threat Working Group and Insider Threat Section, which are responsible for developing

---

[6] Cassandra Lucaccioni, "61st Terrorist Plot Against the U.S.: Terry Lee Loewen Plot to Attack Wichita Airport," *The Issue Brief*, no. 4110 (December 2013), http://www.heritage.org/research/reports/2013/12/terry-lee-loewen-terrorist-plot-in-wichita-kansas-airport.

[7] "Terror Plot BA Man Rajib Karim Gets 30 Years," *BBC News*, March 18, 2011, http://www.bbc.com/news/uk-12788224.

[8] Katko, *America's Airports*, 9.

[9] Deffer, *Transportation Security Administration*, 28–29.

an integrated strategy for addressing these threats. TSA also performs airport vulnerability assessments and monitors information technology systems for indicators of insider threat behavior. Finally, TSA conducts name-based vetting for criminal or terrorism records for all TSA employees and aviation workers. The gap in these measures is that despite initial and recurring employee vetting, some insider threats are not being detected during the planning stages. It is worth considering whether more can be done to detect radicalized or criminal insiders before they have a chance to act. More specifically, is there a role for counterintelligence in TSA's insider threat programs?

The literature reveals that I&A, the FBI, and Lockheed Martin are operating or developing internal counterintelligence programs to mitigate insider threats. Counterintelligence is inherently an offensive measure as compared to security programs, which are defensive in nature. Additionally, counterintelligence is often clandestine activity conducted for national security purposes against a target with suspected or known affiliations with a foreign intelligence service or foreign persons, or an international terrorist organization.[10] Some of the more aggressive counterintelligence measures include double-agent operations and controlled source operations with the intent to collect intelligence on a target.[11]

Ultimately, the research demonstrates there are three key aspects of a model insider threat program: security, counterintelligence, and organizational culture. One of the weaknesses of the TSA insider threat program is its focus on detection and response. The program assumes there will be an ideologically or criminally driven individual lurking in the shadows and waiting for an opportunity to leverage legitimate employee access to further a plot. While this scenario is plausible, TSA's program tends to ignore the ability of an organization's cultural factors to prevent an insider threat from acting due to an established security awareness ethos. CPNI and Lockheed Martin are two organizations that heavily emphasize an organizational culture of security awareness as an insider threat mitigation cornerstone.

[10] Exec. Order No. 12333, 46 Fed. Reg., 3 CFR, § 2.4 (1981), https://www.archives.gov/federal-register/codification/executive-order/12333.html, 24.

[11] Mark L. Reagan, ed., *Terms and Definitions of Interest for Counterintelligence Professionals* (Washington, DC: Department of Defense, 2014), 52.

This research also suggests the first goal of an insider threat program should be prevention by not employing someone who poses an insider threat in the first place. The next goal is to deter the insider threat from acting through the perceived likelihood of discovery. Finally, if an insider cannot be deterred, TSA should have the ability to detect and investigate the insider threat. A comprehensive insider threat program must incorporate all three of these goals.

Successful insider threat programs require a strong balance between security, counterintelligence, and organizational culture. The end goal should be to intersect security and counterintelligence programs. In the words of Robert Hanssen, arguably the most damaging American spy for the Soviet Union, "CI [counterintelligence] attacks the actor. It attacks the opposition intelligence structure. It is not speculative. CI feeds security because it helps them focus on meaningful measures and safeguards. Using CI to help security is just smart security."[12] This thesis recommends focusing on identifying methods for TSA to develop a counterintelligence program, creating a more visible security presence in the SIDA areas of the airport, and improving the security ethos among TSA employees and aviation workers.

[12] Mark L. Reagan, *Introduction to U.S. Counterintelligence-CI 101, a Primer* (Washington, DC: U.S. Department of Defense, 2005), 11.

ACKNOWLEDGMENTS

I would like to thank my family for all of their support over the past 18 months. Jodi, your encouragement and strength has again proven to be the foundation for my success. For Tyler, Lucy, and Trevor, thank you for all your questions and gentle encouragement of me to go “back to school” while you were starting your own academic and life journeys. I deeply regret missing the baseball games, soccer games, dance classes, and first words. A lifelong endeavor of academic pursuit is of utmost importance to me, and I hope you come to the same understanding on your own someday as well.

I must also express a debt of gratitude to my thesis advisors, Ms. Lynda Peters and Dr. Erik Dahl. You both stuck with me even when you were probably scratching your head reading some of the first drafts. Finally, special thanks to Scott Martis, our operations coordinator, for all your assistance and encouragement.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

According to Congressman John Katko, member of the House Homeland Security Committee,

> There is a vast network of approximately 450 airports in the United States that are under federal supervision and control. They serve as a critical component of America's economy connecting people and goods from rural and urban communities across the United States and the world.[1]

This thesis discusses the impact that an insider with nefarious intent can have on the American aviation system and the problem space surrounding the "insider threat." It also provides recommendations for mitigating this threat in the domestic aviation system.

A. PROBLEM STATEMENT

The Transportation Security Administration (TSA) defines insider threat as "one or more individuals with access and/or insider knowledge that allows them to exploit the vulnerabilities of the nation's transportation systems with the intent to cause harm."[2] A well-placed insider is uniquely positioned to conduct espionage, illegal smuggling, and terrorist attacks.

The severity of this threat to the domestic aviation system is significant. A notable terrorism case involving an insider threat is that of Terry Lee Loewen in Wichita, Kansas. In 2013, Mr. Loewen was an avionics technician at Mid-Continent Airport and used his insider access to attempt to detonate a vehicle borne improvised explosive device at the passenger terminal from the secure (runway) side of the airport.[3] Another example is the 2009 case of Rajib Karim who worked as an information technology employee with British Airways and was in regular contact with an overseas, American al-Qaida terrorist

---

[1] John Katko, *America's Airports: The Threat from Within* (Washington, DC: House Homeland Security Committee, 2017).

[2] Frank Deffer, *Transportation Security Administration Has Taken Steps to Address the Insider Threat but Challenges Remain* (Washington, DC: U.S. Department of Homeland Security, Office of the Inspector General, 2012), 2.

[3] Cassandra Lucaccioni, "61st Terrorist Plot Against the U.S.: Terry Lee Loewen Plot to Attack Wichita Airport," *The Issue Brief*, no. 4110 (December 2013), http://www.heritage.org/research/reports/2013/12/terry-lee-loewen-terrorist-plot-in-wichita-kansas-airport.

leader of significant stature. Mr. Karim used his insider access to identify vulnerabilities and opportunities to attack the aviation system, including the recruitment of baggage handlers to place an explosive device onboard an aircraft bound for the United States.[4] In yet another example, in 2014, Mark Quentin Henry (an employee with Delta Airlines) smuggled 153 firearms on 17 different flights between Atlanta and New York City by using his employee access to avoid scrutiny. Henry was assisted by three other airline employees to further his criminal activity.[5] These cases illustrate the severity of the insider threat to the domestic aviation system.

This thesis examines TSA's current policies for identifying and mitigating insider threats within the domestic aviation system and evaluates their overall effectiveness. Simply stated, it studies whether TSA's current insider threat program is effective at identifying, mitigating, and preventing insider threats. TSA addresses insider threat issues through a variety of security measures. These measures include the establishment of an agency-wide Insider Threat Working Group and Insider Threat Section responsible for developing an integrated agency-wide strategy to address these threats. TSA also performs insider threat vulnerability assessments and monitors information technology systems for indicators of insider threat behavior. Other measures include name-based vetting of all TSA, airline, airport, and airport vendor employees. Finally, TSA has also implemented an agency-wide training program to further employee awareness of this threat.[6]

According to the National Counterintelligence and Security Center (NCSC), "(t)he solutions to countering adversarial threats often lie at the intersection of the CI and security disciplines."[7] The NCSC places "insider threat" in the middle of this intersection. CI refers to counterintelligence and is defined in §3001 of Title 50 of the United States Code as:

---

[4] "Terror Plot BA Man Rajib Karim Gets 30 Years," *BBC News*, March 18, 2011, http://www.bbc.com/news/uk-12788224.

[5] Katko, *America's Airports*, 9.

[6] Deffer, *Transportation Security Administration*, 28–29.

[7] "How We Work," accessed October 15, 2016, National Counterintelligence and Security Center, https://www.dni.gov/index.php/ncsc-how-we-work.

> …information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities.[8]

There is both an offensive and defensive aspect to insider threat programs, and identifying these measures and the difference between defensive (protection) and offensive (exploitation, deception, disruption)[9] measures will help identify the most appropriate strategy to deal with insider threats within the domestic aviation system.

B. RESEARCH QUESTION

Primary research question: Is TSA's current insider threat program successful at identifying and mitigating insider threats?

Sub question: Does TSA require additional intelligence collection authorities to improve its ability to mitigate insider threats?

C. LITERATURE REVIEW

This review is an evaluation of the available literature concerning the problem space surrounding the insider threat issue as it relates to the domestic aviation system. It includes resources on security and CI programs commonly used to mitigate insider threats. Much of the reviewed literature is derived from government Office of Inspector General (OIG) reports regarding the U.S. Department of Homeland Security (DHS) and the TSA as well as other aviation sector reports, Naval Postgraduate School theses, executive orders, press releases, and other professional journals. This thesis also reviews government websites in the United Kingdom to identify Military Intelligence Section 5's (MI5's) insider threat policies. For interpretation of legal justifications, I also reference § 3001 of Title 50 of the United States Code, focusing on the set of laws authorizing specific government agencies to participate in "quintessential intelligence activities such

[8] War and National Defense, U.S.C. Title 50 § 3001 (2011), 437.

[9] Ibid.

as intelligence collection and covert action."[10] When appropriate, this thesis covers open source media outlets are cited since some of the insider threat events more thoroughly in open sources. It is appropriate to separate this literature review into two categories: the types of insider threats and policies and methods for insider threat mitigation.

1. What Are the Types of "Insider Threat?"

The term "insider threat" can have different meanings depending on the context (and agency) in which it is used. For this literature review, the TSA definition serves as the primary characterization of the term "insider threat," unless otherwise specified. As noted above, "TSA defines an insider threat as one or more individuals with access or insider knowledge that allows them to exploit the vulnerabilities of the nation's transportation systems with the intent to cause harm."[11] More specifically, TSA identifies many types of insider threat activities, including spying, unauthorized and damaging releases of information, sabotage, corruption, theft, smuggling, impersonation, and terrorist attacks.[12] Most of the literature uses a similar definition in terms of an insider threat's access, but there are sharp differences in which category different agencies emphasize. This thesis discusses four primary areas of concern: an insider that divulges large amounts of electronic data; an insider that smuggles illicit materials onto an airplane; an insider stealing classified information on behalf of a foreign intelligence entity; and insiders seeking to leverage their access to facilitate or conduct a terrorist attack.

The most current literature (2005 to present) tends to focus heavily on the first concern, the threat from an insider with access to sensitive electronic data. This is undoubtedly due to the theft and revelation of enormous amounts of classified information from government information technology systems by Edward Snowden and

[10] Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, Public Law and Legal Theory Research Paper Series (Austin, TX: University of Texas School of Law, 2012).

[11] Deffer, *Transportation Security Administration*, 2.

[12] Ibid.

Bradley (Chelsea) Manning. U.S. government documents often are the best examples for elucidating this bias.

In a statement to the House Homeland Security Subcommittee on Counterterrorism and Intelligence in July of 2016, the then DHS Office of Intelligence and Analysis' Undersecretary, Francis Taylor, described the DHS insider threat program as a "department-wide effort to protect classified national security information from unauthorized disclosure."[13] More specifically, "(t)he purpose of the program is to identify, detect, deter, and mitigate the unauthorized disclosure of classified information."[14] In Frank Deffer's report in 2012, he outlines the steps TSA has taken to address insider threats.[15] The focus of this report is almost entirely on the vulnerability of TSA information technology systems to insider threats. Analysis of the organizational effectiveness at addressing this threat is commonplace in this arena of government OIG reports. Reports of this nature follow the format of identifying the issue, analyzing an organization's programmatic structure to address the issue, providing an agency report card, and finally, providing recommendations for improvement.

Literature specifically discussing insider threats to IT systems is not robust, and when discussed as part of a broader security concern, the literature is recent. Often, the information can be found in other theses and government reports and congressional testimony. The specifics on how an information technology insider can impact the aviation system are unexplored here. For example, could an insider cause enough confusion within an air traffic control system to result in a catastrophic loss of life and/or property? This topic appears to be a significant information gap in the literature.

In contrast, the Federal Bureau of Investigation (FBI) defines "insider threat" as an individual with authorized access who steals information to sell and/or provide to a foreign government. It warns "(t)hat an insider may steal solely for personal gain, or that

---

[13] Francis Taylor, Robert Hayes, and Rich McComb, *Counterintelligence and Insider Threats: How Prepared Is the Department of Homeland Security?* (Washington, DC: Department of Homeland Security, 2016), 6.

[14] Ibid.

[15] Deffer, *Transportation Security Administration*.

an insider may be a 'spy'—someone who is stealing company information in order to benefit another organization or country."[16] Unlike DHS, the FBI's focus with insider threats is the theft of sensitive technology and proprietary data to sell or benefit another organization or country. Most of the FBI literature describing its role in this field focuses on foreign intelligence services attempting to steal secrets.

There is somewhat of a gap in the insider threat as a "terrorism issue" school of thought as well. The literature in this area is primarily from open sources and lacks the established government analysis and OIG evaluations as the other schools of thought (CI problem). Although less prevalent than criminal insider threats, a terrorist with insider access is uniquely positioned to cause catastrophic damage and loss of life within the aviation system.

There are a few present-day examples of successful terrorist attacks involving insider threats in the aviation system since 2015. For instance, on February 2, 2016 in Mogadishu, Somalia, insiders working as airport security employees coordinated the passage of an explosive filled laptop through a security checkpoint x-ray machine. Soon after, the insiders passed the laptop to a passenger boarding Daallo Airlines flight 159, and he later detonated it onboard this flight. This attack was immediately claimed by al-Shabaab, a terrorist group based in east Africa.[17] Another example occurred on October 31, 2016, when a bomb detonated on board Russian airliner Metrojet 9268, causing the plane to crash approximately 20 minutes after takeoff. Russian investigators believe a baggage loader loyal to the Egyptian offshoot of Islamic State of Iraq and the Levant (ISIS) placed the bomb directly on the plane.[18] Although these events took place internationally, both examples are indicative of the intent and capability of international terrorist groups which homegrown violent extremists in the United States have joined or

---

[16] Federal Bureau of Investigation, *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy* [brochure] (Washington, DC: Federal Bureau of Investigation, 2011), https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view.

[17] Kylie Bull and Ben Vogel, "Daallo Airlines Bombing Investigation Focuses on Insider Threat," *IHS Jane's 360*, February 9, 2016, http://www.janes.com/article/57845/daallo-airlines-bombing-investigation-focuses-on-insider-threat.

[18] Owen Mathews, "Metrojet Crash: Why The Insider Threat to Airport Security Isn't Just Egypt's Problem," *Newsweek*, May 24, 2016, http://www.newsweek.com/2016/06/03/egyptair-metrojet-flight-9268-airport-security-462784.html.

been inspired by. The vulnerability from a sympathetic insider presents a similar risk in the United States as it does overseas, regardless of security measures due to employees' unique access and ability to circumvent security measures.

Due to the recent nature of these events, they are not included in many theses related to aviation security or insider threats. However, a large amount of media from western newspapers and newsmagazines is available concerning these events and can be used to corroborate information to paint an accurate picture of these events. For example, these incidents are all covered in depth by the *BBC News*, *CNN*, *Washington Post*, *New York Times*, and other such publications.

The literature discussing criminal insider threats to the domestic aviation system is significantly more robust than the literature describing insider threats tied to terrorism. Sources describing incidents of criminal activity involving insider threats are plentiful in both open source reports as well as journal articles, but government reports are less available. However, one could argue that an insider with motive, means, and opportunity for terrorist pursuits would take advantage of the same vulnerabilities as exploited by criminals.

Criminal activity can be separated out into many different categories, such as trespass, theft, drug trafficking, human smuggling, weapons smuggling, etc. In one of the more prominent examples, in March 2007, two airline employees trafficked 14 guns and "eight pounds of marijuana on board a commercial airplane at Orlando International Airport"[19] in Florida. Another critical event leading to significant changes in TSA's screening procedures for airport employees is the previously mentioned gun smuggling ring involving Mark Quentin Henry in 2014.[20] This event led to multiple congressional inquiries and industry recommendations.

---

[19] U.S. Government Accountability Office, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Perimeters and Access Controls* (Washington, DC: U.S. Government Printing Office, 2009), 2.

[20] Joe Sharkey, "Gun Smuggling on Plane Reveals Security Oversight," *The New York Times*, December 29, 2014, http://www.nytimes.com/2014/12/30/business/gun-smuggling-on-plane-reveals-security-oversight.html?_r=0.

In contrast, the government of the United Kingdom strikes a different tone when discussing insider threats. Its overall focus is more about establishing a sound policy and model than on the specifics of what an insider threat is (terrorist, criminal, spy, etc.). For example, the United Kingdom's official government agency website on this issue identifies the Centre for Protection of National Infrastructure (CPNI), part of MI5, as the "government authority for protective security advice to the United Kingdom national infrastructure."[21] Links on the page include United Kingdom CPNI studies on the data pertaining to what factors motivate insider threats instead of their end goal. In short, the emphasis is behavior-focused and attempts to create a profile for different types of insider threats. According to CPNI, there are five chief types of insider threat behaviors: unauthorized revelation of information, process corruption, the enabling of outside entity access, physical sabotage, and electronic interference.[22] This contrasts with the OIG and U.S. government documents that tend to focus more on the individual's end game (intent) as the main threat instead of potential avenues for the illicit activity.

2. Policies and Methods for Insider Threat Mitigation

In Frank Deffer's OIG report, *Transportation Security Administration Has Taken Steps to Address the Insider Threat but Challenges Remain,* he discusses this issue from a policy and procedures viewpoint. Deffer analyzes TSA's internal structure to address and investigate insider threats, and he suggests TSA still needs to increase its ability to centrally monitor all information systems to better detect an attempt by an insider to illicitly extract large amounts of data onto removable media devices.[23] The 2008 OIG report titled *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening* takes a slightly different view. This report argues that 100 percent screening of employees in the

[21] "About CPNI," Centre for the Protection of National Infrastructure, accessed October 15, 2017, https://www.cpni.gov.uk/about-cpni.

[22] Centre for the Protection of National Infrastructure [CPNI], *CPNI Insider Data Collection Study: Report of Main Findings* (London: Centre for the Protection of National Infrastructure, 2013).

[23] Deffer, *Transportation Security Administration*, 13.

sterile area (past checkpoint screening) is unfeasible due to resource constraints and the burden placed on these employees.[24]

Another argument explored by a 2012 OIG report is found in *Efficiency and Effectiveness of TSA's Visible Intermodal Prevention and Response Program (VIPR) within Rail and Mass Transit Systems*. Although the title indicates otherwise, this article discusses using TSA high visibility operations in the sterile area of the airport as a method to deter insider threats. This operation includes multiple TSA employees, often including armed federal air marshals, conducting high visibility security procedures in a random and unpredictable manner.[25] This represents a dissenting opinion in the literature already and argues for a proactive, visible deterrent as an excellent means for mitigating insider threats. The Deffer OIG report, on the other hand, argues for a more robust information technology monitoring capability that is essentially a passive, defensive security measure.

Others believe the best solution to mitigating the insider threat is in the employee background check process conducted by each airport. In his 2010 Naval Postgraduate School thesis entitled "Managing the Aviation Insider Threat," Alan Black recommends airports further leverage and enhance the background check of a prospective employee. He argues for more frequent criminal records checks and criminal prosecution for those that do not self-report a conviction within 24 hours (as is required by law). Moreover, he would like to see this taken a step further and require self-reporting of arrests.[26] Although Black argues for putting "more teeth" into the vetting process, he is still advocating for more aggressive defensive measures. In this case, the defensive measure is reliant upon the cooperation of employees to report information that might be detrimental to their employment. Even more far-fetched is the idea that insiders with nefarious intent would provide self-reporting and derail their own plot.

---

[24] War and National Defense, U.S.C. Title 50 § 3001 (2011).

[25] Charles K. Edwards, *Efficiency and Effectiveness of TSA's Visible Intermodel Prevention and Response Program Within Rail and Mass Transit Systems* (Washington, DC: U.S. Department of Homeland Security, Office of the Inspector General, 2012).

[26] Alan Black, "Managing the Aviation Insider Threat" (master's thesis, Naval Postgraduate School, 2010).

Lockheed Martin identifies defensive measures within its insider threat program but also advocates for a much more proactive CI approach to the problem. Its Director of CI Operations and Investigations, Douglas Thomas, considers the entire spectrum of defensive and offensive insider threat mitigation measures to fall under the CI umbrella, and the company manages each of these measures by a cadre of experience CI professionals.[27] He argues against profiling as a mitigation measure and uses "red team" exercises designed to test defensive measures. This is in stark contrast to the United Kingdom, in which its lead agency, CPNI (under MI5's hierarchy), advocates for using various profiling and behavioral analysis measures to detect insider threats.[28]

There are some advocates for a more holistic approach to the issue as well. Lockheed Martin and CPNI both advise for robust measures at the pre-employment screening stage up until the employee leaves the company or agency. According to CPNI, "Using robust and on-going protective security measures and establishing effective management practices is key to reducing vulnerability."[29] It identifies good management practices as a critical element of creating a loyal and committed workforce and minimizing feelings of disgruntlement.[30] This emphasis on management's role does not appear in the literature describing TSA's insider threat programs or in the various OIG reports' recommendations.

Another counterargument to passive insider threat detection (waiting for malicious activity to occur) is for organizations to use behavior modeling. Sources advocating for this approach were mostly published between 2003–2010. This approach argues illicit insiders are a "people" problem and countermeasures should emphasize profiling and discovering irregularities in employee behavior. According to Puleo in a 2006 paper, "The new risk-based model focuses on observable influences that affect

---

[27] Douglas D. Thomas and Harvey Rishikof, "Counterintelligence and Insider Threat Detection" (presentation for Government Contractors Forum, Security Clearance and Insider Threat Boot Camp, February 2016), http://m.acc.com/chapters/ncr/upload/Session-2-Insider_Threat_Program_Panel2_020916.pdf.

[28] "About CPNI," Centre for the Protection of National Infrastructure.

[29] CPNI, *CPNI Insider Data Collection*, 15.

[30] Ibid., 15.

employees and identifies employees with increased risk of becoming malicious insiders."[31] Although the most recent literature indicates TSA has shied away from using a behavior modeling strategy, this approach does represent a proactive approach to identifying employees with possible malicious intent and has value in the broader debate. CPNI also favors the behavior modeling approach to insider threat mitigation. It has identified four behaviors of interest when frequent behavior trends are noted without an adequate explanation: engaging in unusual copying activity, unusual information technology activity, unauthorized handling of sensitive material, and committing security violations.[32]

3. Conclusion from the Literature

The literature discussing insider threats to the aviation system has significant gaps and is somewhat disjointed. In addition to some of the holes identified in the body of this literature review, there is also very little legal analysis on what measures TSA can or cannot additionally implement to more aggressively mitigate the insider threat. It is unclear at this point if this is solely due to a lack of literature, a lack of urgency, or a lack of overall concern. On the other hand, OIG and GAO reports provide an excellent backbone of credible material discussing TSA current programs to mitigate insider threats. These materials focus primarily on employee vetting against terrorism databases as well as information technology monitoring to detect suspicious activity.

Another key gap in the literature appears to be the discussion on rights and authorities for more aggressive law enforcement or intelligence collection measures within TSA to counter the insider threat. This seems to be a largely unexplored topic, and it is not clear if this is due to a lack of granted authority to conduct such activities or a lack of attempt to do so by a relatively new federal agency such as TSA. It appears this is a question that will force an answer soon as the threat will drive agency action. Perhaps the solution is for the DHS Office of Intelligence and Analysis (I&A) to assume this

[31] Anthony J. Puleo, "Mitigating Insider Threat Using Human Behavior Influence Models" (master's thesis, Air Force Institute of Technology, 2006).

[32] CPNI, *CPNI Insider Data Collection*, 12.

responsibility over the aviation system as a Title 50 organization with CI and intelligence collection authority. Maybe current authorities assigned to TSA can be interpreted to allow TSA to develop more intrusive offensive collection measures to identify insider threats. These are research questions worth exploring further and represent a knowledge gap in the available literature.

D. RESEARCH DESIGN

This thesis utilizes a policy options analysis framework to identify the current policies within TSA for mitigating insider threats, shortcomings of TSA's current policies, and policy recommendations for improving TSA's ability to counter these threats. For the purpose of identifying alternative solutions, it is important to compare how other government agencies and companies mitigate insider threats. I compare the insider threat policies of the FBI, DHS I&A, Lockheed Martin, and MI5/CPNI (United Kingdom).

This thesis explores the applicability, legality, and effectiveness for TSA to conduct more intrusive, offensive CI collection. CI has traditionally been directed at foreign intelligence entities, but could it also be directed at mitigating a drug smuggler working for a domestic airline? The FBI has an established domestic CI mission and law enforcement function, and as the lead domestic CI agency its policies for addressing insider threat provide an excellent analytical comparison as well.[33] Comparing the policies and authorities used by other entities to conduct CI operations is useful in determining the best policy recommendations for TSA.

Inevitably, some of the more intrusive measures require an analysis of whether TSA can legally conduct certain operations, especially when U.S. persons (citizens or lawful permanent residents) are involved. Since most offensive measures are CI collection operations, it is prudent to consider if TSA can legally conduct such operations, and, if not, what additional authority it would require.

[33] War and National Defense, U.S.C. Title 50 § 3001 (2011), 435.

E. THESIS OVERVIEW

The next chapter of this thesis is a description of TSA's current insider threat mitigation policy and an analysis of the effectiveness of TSA's insider threat program. To provide alternative policy options, Chapter III describes the insider threat policies of the FBI, I&A, Lockheed Martin, and the United Kingdom's MI5/ CPNI. Chapter IV compares and analyzes the insider threat policies of these entities and discusses various courses of action TSA can consider adapting to improve its insider threat programs. The last chapter provides final policy recommendations for TSA to improve its insider threat programs based on the analysis within this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE TRANSPORTATION SECURITY ADMINISTRATION'S INSIDER THREAT PROGRAM

> The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) and the Federal Bureau of Investigation (FBI) have characterized the threat of rogue aviation workers, who exploit their credentials, access, and knowledge of airport security procedures for personal gain or to inflict damage—referred to as the insider threat—as one of aviation security's most pressing concerns.[34]

A. INTRODUCTION

TSA plays a critical role in the everyday lives of Americans as the federal agency primarily responsible for ensuring the freedom of movement for both people and commerce on the homeland's transportation systems. TSA was created in November 2001 when Congress passed the Aviation and Transportation Security Act of 2001 (ATSA). The ATSA assigned TSA responsibility for security in all modes of transportation, including aviation, maritime, mass transit, highway, freight rail, and pipeline. The transportation sector is often privately owned, and therefore TSA collaborates with industry and other levels of government to assist these entities in securing their systems.[35] In the aviation sector, TSA screens passengers, baggage, and cargo to prevent acts of terrorism.[36] The ATSA also charges TSA with improving airport perimeter and access control to the secured areas of airports while reducing the security risks posed by workers at these airports.[37]

This chapter discusses the scope of the insider threat within the domestic aviation system and TSA's current policies and methods for mitigating this threat. TSA is primarily playing defense with its insider threat mitigation methods, and it operates within the framework of protective security programs. Security programs are designed to

---

[34] Jennifer A. Grover, *Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates* (Washington, DC: U.S. Government Accountability Office, 2016).

[35] "TSA Mission," Transportation Security Administration, accessed April 29, 2017, https://www.tsa.gov/about/tsa-mission.

[36] Deffer, *Transportation Security Administration*, 2.

[37] U.S. Government Accountability Office, *Aviation Security*.

protect against unauthorized access, both physical and virtual. As a metric for success, prevention is difficult to measure. However, this chapter reviews and analyzes insider threat cases within the domestic aviation system that current TSA security programs failed to prevent or identify. The conclusion of this chapter addresses the overall success of TSA's insider threat program. It also considers whether TSA should adopt offensive insider threat mitigation measures. More specifically, is there a role for CI in TSA's insider threat program?

B. SCOPE OF THE INSIDER THREAT ISSUE WITHIN THE DOMESTIC AVIATION SYSTEM

According to an Airports Council International of North America study, about 1.2 million people work at 485 commercial airports in the United States.[38] Numbers from TSA in 2015 indicate approximately 440 of these airports are federalized. A 2017 House Homeland Security Committee report cites approximately 900,000 aviation workers at approximately 450 federalized airports.[39] A federalized airport must meet specified regulatory requirements and TSA standards for security, screening, and access control.[40] Although there is some fluctuation in numbers, it is reasonable to consider there are approximately one million aviation workers comprising the potential of an insider threat.

In the aviation environment, possible insider threats include TSA employees, airline workers, airport vendors, and airport contractors with access to areas restricted to the public. This cadre of airline workers, airport workers, airport vendors, and contractors are collectively referred to as "aviation workers" by TSA. Many of these aviation workers are granted secure identification display area (SIDA) badges giving them physical access to many of the most sensitive areas of an airport, including planes on the runway and passenger baggage transiting areas.[41] TSA employees alone account for over 50,000 aviation workers nationwide with access to sensitive areas and information at

[38] Harriet Baskas, "How Many People Does It Take to Run an Airport?," *USA Today*, March 30, 2016, https://www.usatoday.com/story/travel/flights/2016/03/30/airport-workers-employees/82385558/.

[39] Katko, *America's Airports*, 2.

[40] Grover, *Aviation Security*, 8.

[41] John Roth, *TSA Can Improve Aviation Worker Vetting* (OIG-15-98) (Washington, DC: U.S. Department of Homeland Security, Office of Inspector General, 2015), 8.

domestic airports. Herein lies the potential of insider threat within the aviation system from both TSA employees and other aviation workers. Trusted insiders are usually familiar with weaknesses in internal policies and procedures, physical security code procedures, and information technology systems.[42]

A 2017 House Homeland Security Committee majority staff report on insider threats within American airports revealed Congress remains concerned that insider threats in the aviation system are rising.[43] TSA and the FBI agree insider threats represent one of aviation security's "most pressing concerns."[44] These agencies have identified access controls to sensitive areas at airports as a significant source of vulnerability within the aviation system. In terms of employee and aviation worker vetting, TSA has significant gaps in the data sets it has been granted access to by the U.S. Intelligence Community (IC). This recently resulted in 73 aviation workers, all with jobs requiring some degree of sensitive area airport access, passing TSA vetting checks even though the IC had identified them as having possible ties to terrorism.[45]

C. TSA'S CURRENT INSIDER THREAT POLICIES

TSA has implemented steps to address insider threats, both within its workforce and the broader aviation worker population it is responsible for vetting. As TSA began seriously re-examining insider threat issues back in December 2008, the TSA Office of Inspection began to develop and facilitate an insider threat program. It established an internal Insider Threat Task Force to implement an education and awareness campaign for both TSA employees and aviation stakeholders.[46]

However, the problem has continued to be a major issue for the agency and industry. TSA focuses its efforts on two fundamental areas when it comes to preventing an insider threat who poses a threat from acting. First, how can TSA best conduct

[42] Deffer, *Transportation Security Administration*, 4.

[43] Katko, *America's Airports*, 2.

[44] Grover, *Aviation Security*, 22.

[45] Katko, *America's Airports*, 3–5, 10.

[46] Deffer, *Transportation Security Administration*, 5.

background checks (commonly referred to as "vetting") on an initial and continuing basis to prevent known or suspected terrorists and persons with disqualifying criminal records from gaining insider access? Second, how can TSA regulate and enforce access control to prevent insiders who pose threats from using their employee access to further nefarious activity?

TSA's current vetting requirements and authority are stipulated in Chapter 49 of the Code of Federal Regulations. This requires aviation workers "applying for credentials to work in secure areas of commercial airports undergo background checks prior to being granted badges that allow them unescorted access to secure areas."[47] The background check must include the following:

1. A security threat assessment on the individual from TSA (including database checks for ties to terrorism).
2. Fingerprint-based criminal history records check.
3. Evidence the applicant has a right to work in the United States.[48]

In a 2015 DHS OIG report *TSA Can Improve Aviation Worker Vetting*, the OIG determined TSA does a generally effective job of employing controls for vetting aviation workers and coordinating results with the FBI and National Counterterrorism Center.[49] However, these measures are only effective at identifying *individuals associated with terrorism that we know about already*. This is a key distinction in today's threat environment in which the inspired lone wolf or homegrown violent extremist is an unknown individual committing a terrorist act.

The DHS OIG also "determined that TSA had multiple, layered controls for vetting workers for terrorism."[50] TSA's vetting procedures check aviation workers "against the Consolidated Terrorist Watchlist within minutes of receiving updated watchlist data"[51] for individual aviation workers. When new aviation workers are

[47] Roth, *TSA Can Improve*, 4.

[48] Ibid.

[49] Ibid.

[50] Ibid., 2.

[51] Ibid.

employed, they are immediately vetted against this watchlist, and when there is an update (often these are additions) to watchlist data, nearly one million existing credentialed aviation workers are re-vetted within minutes.[52] This ensures new aviation workers are not currently on the watchlist and if any current aviation workers later added to the watchlist, they are promptly identified as such.

However, the DHS OIG found TSA has significantly less effective controls for ensuring airports "have a robust verification process over a credential applicant's criminal history and authorization to work in the United States."[53] TSA does not perform recurrent criminal records vetting (akin to the recurrent vetting checks for terrorism watchlist records) and airport operators are left to verify criminal histories for disqualifying offenses at the time aviation workers become employed at the airport. Per 49 CFR § 1542.209(e), aviation workers are responsible for self-reporting convictions within 24 hours to the airport operator that issued the secure area access badge.[54] Needless to say, there is a serious conflict of interest for aviation workers to report their own disqualifying offenses once employed as this will likely lead to their loss of employment.[55]

TSA is expanding its use of the FBI Rapback program in aviation worker vetting. This program provides 24/7 vetting of aviation workers and notifies the employing entity of new arrests and other criminal activity that might disqualify them from maintaining their sensitive area access.[56] Although TSA's vetting program is effective at identifying watch-listed individuals (known or suspected terrorists) who become known while they are employed, airport operators have long complained of the absence of such a program when it comes to *criminal records*, which also could be used to determine if an employee is an insider threat to the aviation system.

---

[52] Ibid.

[53] Ibid.

[54] Black, "Managing the Aviation Insider Threat," 35.

[55] Roth, *TSA Can Improve*.

[56] Katko, *America's Airports*, 14.

Many members of Congress recommend that TSA should physically screen 100 percent of aviation workers entering the sterile areas of an airport in order to deter (or identify) an insider threat.[57] In 2007, Congress introduced two bills pursuing the 100 percent aviation worker screening requirement,[58] but neither bill was passed by both bodies of Congress.[59] After the Atlanta gun smuggling incident in 2014 (mentioned above), there were renewed calls for TSA to conduct 100 percent physical screening for aviation workers. However, the concept was widely rejected by both TSA and the aviation industry as generally ineffective. In a 2015 Aviation Security Advisory Committee report, the aviation industry concluded that 100 percent screening did not represent a "silver bullet" and that other more cost effective actions, such as random employee screening, and expanded domestic intelligence collection measures like social media account monitoring, could have a similar effect.[60] Kathleen Rice (D-New York), a ranking member of the Transportation Security Committee, similarly advocates that all aviation workers should come to work with the expectation they will be physically screened that day; however, she acknowledges that 100 percent aviation worker screening might not be the only solution.[61] The plausible expectation of physical screening of the aviation workers and their bags or other items at any time when entering a secured area is considered a critical layer in a *multi-layered* approach to mitigating insider threats.[62]

TSA has resisted adopting a 100 percent aviation worker screening footprint as it is both resource intensive for TSA and time intensive for aviation workers to submit to

---

[57] Aviation Security Advisory Committee, *Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control* (Arlington, VA: Aviation Security Advisory Committee, 2015), 2, 7.

[58] Richard L. Skinner, *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening* (OIG-09-05) (Washington, DC: U.S. Department of Homeland Security Office of Inspector General, 2008), 2.

[59] H.R. Rep. No. 1413 (110th), *To Direct the Assistant Secretary of Homeland Security (Transportation Security Administration) to Address Vulnerabilities in Aviation Security by Carrying Out a Pilot Program to Screen Airport Workers with Access to Secure and Sterile Areas of Airports, and for Other Purposes*, https://www.govtrack.us/congress/bills/110/hr1413.

[60] Aviation Security Advisory Committee, *Final Report*, 2–4.

[61] Scott Zamost and Drew Griffin, "Despite Security Gaps, No Full Screening for Airport Workers," *CNN*, April 21, 2015, http://www.cnn.com/2015/04/20/travel/airport-workers-security-screening/index.html.

[62] Ibid.

daily physical screening. As a result, TSA prefers a policy of targeted, random screening measures for aviation workers. This approach has generally been supported by the aviation industry.[63] Unpredictable and random aviation worker screening measures at prearranged employee entrances can be an effective deterrent if executed appropriately. To be effective, random aviation worker screening resources need to be allocated to cover all employee access points within a specific area and time to prevent aviation workers from entering the secure area through another entrance.[64]

Unfortunately, this has been identified as a weak point in TSA's random screening measures. According to a 2015 Aviation Security Advisory Committee report, "Static security measures, such as physical screening, can be studied, tested, and more easily circumvented than those that are dynamic and less predictable."[65] After all, a random employee screening checkpoint can be rendered ineffective if another employee entrance to the secured access area is available without screening. An insider threat could merely bypass the random employee screening checkpoint and proceed through a different entrance. As a counter measure, the Aviation Security Advisory Committee recommends in 2015 that airport and aircraft operators selectively close adjacent access points during TSA's random screening operations in the secured areas to help funnel aviation workers to TSA's random physical screening checkpoints.[66]

TSA has also taken a number of steps to detect and mitigate insider threats from TSA employees seeking to use their legitimate access to information technology systems to further nefarious insider activities. TSA processes classified and sensitive information on its various information technology systems, and this information could be useful to a foreign government, terrorist group, or criminal enterprise. In the spirit of the creation of national level Insider Threat Task Forces and working groups (mandated by Executive Order [E.O.] 13587), TSA has also established the internal Insider Threat Working Group and Insider Threat Unit to implement multiple insider threat reporting and identification

[63] Aviation Security Advisory Committee, *Final Report*, 2.

[64] Ibid., 2–3.

[65] Ibid., 8.

[66] Ibid., 11.

programs. The Insider Threat Unit is run by the agency's Office of Law Enforcement (comprised of federal air marshals and collaborates with both "state and federal partners to actively monitor criminal activity within airports."[67] According to 2016 testimony from Darby LaJoye, TSA Deputy Assistant Administrator, the Insider Threat Unit's efforts have resulted in several arrests.[68] Vulnerability assessments and integrity checks are also conducted regularly on TSA information technology systems along with a security operations center that monitors the daily activity and security of TSA information technology systems.[69]

TSA has also utilizes a much-scrutinized program over the years called the Visible Intermodal Prevention and Response (VIPR) team to counter insider threats from aviation workers through visible deterrence and unpredictable aviation worker random screening checkpoints.[70] VIPR teams are comprised of federal air marshals, local law enforcement officers, behavior detection officers, explosives detection canine teams, explosives specialists, regulatory inspectors, and transportation security officers or any combination thereof. The original purpose of a VIPR team was to be an unpredictable and visible presence at various transportation modes as a deterrent to terrorist activity. These operations can be considered a more aggressive form of random aviation worker screening operations coupled with a visible law enforcement presence and other TSA security assets. Questions have arisen, however, regarding the program's security value to the transportation industry.

D. SHORTCOMINGS AND SUCCESSES OF TSA'S INSIDER THREAT POLICY

In recent years, several incidents have made it clear the insider threat in the aviation system is a significant problem, and represents a major vulnerability to both

---

[67] Katko, *America's Airports*, 17.

[68] *Securing Our Skies: Oversight of Aviation Credentials: Statement of Darby LaJoye, Deputy Assistant Administrator, Transportation Security Administration, U.S. Department of Homeland Security before the House Oversight and Government Reform Committee, Subcommittee on Transportation and Public Assets* (2016), https://www.tsa.gov/news/testimony/2016/02/03/testimony-hearing-securing-our-skies-oversight-aviation-credentials.

[69] Deffer, *Transportation Security Administration*.

[70] Edwards, *Efficiency and Effectiveness*, 4–5.

criminals and terrorists. Criminal activity involving aviation workers has been a regular occurrence. The gun smuggling ring in 2014 in Atlanta (mentioned in Chapter I) is just one example of an insider event in which multiple airline employees were involved in a sophisticated gun smuggling ring. Orlando International Airport had a similar case back in 2007 when two Comair Airline employees were caught attempting to smuggle eight pounds of marijuana and fourteen firearms onto a Delta Air Lines commercial flight to Puerto Rico.[71]

TSA has also experienced a few employees and TSA contractors who have used their insider access for criminal activity. In February of 2017, the U.S. Attorney's Office for the District of Puerto Rico indicted 12 persons charged with "conspiracy to possess with intent to distribute" cocaine. The cocaine was smuggled through the TSA security system at Luis Muñoz Marín International Airport in San Juan, Puerto Rico. Six current and former TSA employees are included among the 12 people indicted. These employees were transportation security officers who screened both checked and carry-on luggage. The indictment alleges the TSOs cleared luggage filled with cocaine through the X-ray screening machines while another aviation worker safeguarded the bags until they were smuggled onboard an aircraft, thus avoiding any canine or law enforcement patrols.[72]

In another example, at San Francisco International Airport, two TSA security screeners were arrested in 2015 for smuggling methamphetamine through the airport. Both screeners were contractors working as transportation security officers and are alleged to have purposely overlooked pre-specified packages and bags at the security checkpoints in exchange for monetary bribes.[73] In conjunction with the gun smuggling operations in Atlanta and Orlando, these examples demonstrate that TSA, despite federal background checks and vetting, is susceptible to insider threats within its organization.

---

[71] Skinner, *TSA's Security Screening*, 1.

[72] "Twelve Current and Former TSA and Airport Employees Indicted for Smuggling Approximately 20 Tons of Cocaine" press release, U.S Attorney's Office, District of Puerto Rico, February 13, 2017, https://www.justice.gov/usao-pr/pr/twelve-current-and-former-tsa-and-airport-employees-indicted-smuggling-approximatley-20.

[73] "TSA Screeners Accused of Drug Smuggling Conspiracy," *Bay City News*, March 6, 2015, http://abc7news.com/news/tsa-screeners-accused-of-drug-smuggling-conspiracy/548594/, sec. News.

Unfortunately, there have also been multiple incidents involving known or suspected terrorists and their very troubling prior employment as aviation workers at domestic airports before their involvement with terrorist attacks overseas. These events have shined a particularly bright spotlight on the Minneapolis-St. Paul International Airport in Minnesota. In October of 2008, Shirwa Ahmed became the first known suicide bomber from the United States to join al-Shabaab, a terrorist organization in Somalia aligned with al-Qaida. Ahmed was an airport cart driver at Minneapolis-St. Paul International Airport before leaving for Somalia to join al-Shabaab.[74] Although this incident took place prior to TSA's 2008 revamp of its insider threat programs, it is noteworthy to point out that TSA's insider threat program has continued to have difficulty with identifying radicalized individuals. Another suicide bomber who once worked at Minneapolis-St. Paul International Airport was killed fighting for al-Shabaab in Somalia in October of 2011. Abdisalan Hussein Ali, another radicalized aviation worker, served coffee in the airport across from a Customs and Border Protection checkpoint before heading overseas to fight for al-Shabaab.[75] Additionally, in November of 2014, three more men who once worked at Minneapolis-St. Paul International Airport were recruited to fight for ISIS in Syria and Iraq. One of these three men, Abdirahmaan Muhumed, cleaned the interior of arriving planes and refueled them on the ramp. He had a SIDA badge granting him direct access to airplanes on the runway.[76]

It is important to note these terrorists did not conduct attacks during their employment at the Minneapolis-St. Paul International Airport. However, it is concerning that they were radicalized or in the process of being radicalized while they were aviation workers with SIDA access. None of the security measures (primarily vetting) identified these aviation workers as either known or suspected terrorists. This is even more

[74] Peter Bergen, "How Big of a Threat Is Al-Shabaab to the United States?" *CNN*, February 22, 2015, http://www.cnn.com/2015/02/22/opinion/bergen-al-shabaab-threat/index.html.

[75] Katko, *America's Airports*, 8.

[76] Ibid.

concerning today as ISIS has encouraged radicalized individuals to conduct attacks abroad as the group loses territory in Syria and Iraq.[77]

Also alarming is that just a year later, in December of 2015, Moniteveti Katoa, an aviation worker at Dallas-Ft. Worth International Airport in Texas, told an undercover FBI agent he could smuggle explosives onboard an aircraft for a $4,000 fee.[78] Katoa led a group of three other aviation workers in a cocaine smuggling operation prior to his arrest. His willingness to smuggle explosives is a foreboding example of the seriousness the insider threat vulnerability poses to the aviation system.[79] Whether motivated by ideology or profit, terrorists and criminals have been able to gain employment within the domestic aviation system. Although Katoa was eventually discovered and arrested, one could argue TSA's insider threat program failed to prevent Katoa from leading a small cocaine smuggling ring; however, it can be considered a success that Katoa was eventually identified and arrested by the FBI.

In testimony to Congress in February of 2016, TSA stated, "that recent insider threat mitigation efforts have yielded arrests in Dallas, Los Angeles, San Francisco and Puerto Rico."[80] These arrests have been linked to coordination and referrals by the TSA Insider Threat Unit to other federal law enforcement agencies.[81] Specific details on the TSA Insider Threat Unit's role in the arrests are not publicly available, and one can assume this is to protect the sources and methods by which the insider threats are identified.

It is clear, however, that TSA's employee and aviation worker vetting programs have not been able to identify a number of insider threats. A major part of the problem is

---

[77] Associated Press, "ISIS Leader Encourages Lone Wolf Attacks on Civilians in Europe and U.S.," *The Guardian*, May 22, 2016, https://www.theguardian.com/world/2016/may/22/isis-leader-civilian-lone-wolf-attacks-us-europe.

[78] Katko, *America's Airports*.

[79] "Dallas Man Sentenced to 188 Months in Federal Prison for Role in Conspiracy to Transport, or Assist in Transporting, a Substance Represented to Be Cocaine on Flights from DFW Airport as Part of an Undercover Law Enforcement Operation," press release, U.S. Attorney's Office Northern District of Texas, September 22, 2016, https://www.justice.gov/usao-ndtx/pr/dallas-man-sentenced-188-months-federal-prison-role-conspiracy-transport-or-assist.

[80] Katko, *America's Airports*, 9.

[81] Ibid., 17.

these security programs are defensive in nature with a heavy emphasis on initial and recurrent vetting. These programs are used to identify known or suspected terrorists or persons with disqualifying criminal records prior to or during their employment with TSA or as aviation workers. The weakness in these programs is they can only identify known criminals and known or suspected terrorists *after* they have already come in contact with law enforcement or intelligence personnel. In other words, these are all persons we know about and can perform an individual threat assessment on to determine their level of risk to the aviation system. Nevertheless, the insiders who pose successful threats is the one that TSA did not know about prior to their employment, and their criminal or terrorist activity remains undetected during their employment.

The gap in the system is that despite pre- and post-employment vetting, some insider threats are not being detected during the planning stages of their nefarious activity. It is worth considering if more can be done to detect radicalized or criminal insiders before they have a chance to act, but the challenge remains detecting individual intent. This is not a new problem and many U.S. government agencies have tried various methods to fill in this gap and identify insiders who pose threats before they can cause too much damage. There are a wide range of options to consider such as organizational cultural changes, clandestine source operations, domestic intelligence collection, and even polygraph exams.

E. SHOULD TSA ADOPT OFFENSIVE INSIDER THREAT MITIGATION MEASURES?

The *National Insider Threat Policy* requires all federal executive branch agencies to "establish a program for deterring, detecting, and mitigating insider threat; leveraging CI, security, information assurance, and other relevant functions and resources to identify and counter the insider threat."[82] When applied to the TSA operating space under the Title 50 definition, CI can be described as actions taken to protect against espionage, sabotage, and international terrorism activities.[83]

---

[82] White House, *National Insider Threat Policy* (Washington, DC: White House, 2012).

[83] War and National Defense, U.S.C. Title 50 § 3001 (2011), 437.

CI is inherently an offensive measure when compared to security programs. It is often clandestine activity conducted for national "security purposes against a target having suspected or known affiliation"[84] with a foreign intelligence entity or international terrorism. Some of the more aggressive CI measures include double agent operations and controlled source operations with the intent to collect intelligence on a target. There are also less intrusive CI measures, such as technical surveillance countermeasures and employee polygraphs, which are designed to protect an agency's resources from collection or exploitation by a foreign intelligence service.[85]

The difference between security and CI is nuanced but critical to distinguish. Stated simply, CI is not security. Security only protects, but as an offensive tool, CI attacks and goes beyond the defensive nature of security. Security functions include physical (facility and personnel) protection, personnel background checks/investigations, information technology systems security, document control, education, and awareness training. The main threat concern with security is unauthorized access. In contrast, the main threat concern with CI is clandestine and covert threats. Insiders posing threats span the spectrum of CI and security because they utilize clandestine and covert action while capitalizing on employee access to get around physical and virtual access controls.[86] In fact, insiders often bypass the security disciplines because they have authorized access to sensitive areas and systems by nature of their employment.

TSA does not make any claim concerning the conduct of CI operations, and there is no description of a CI program in any of the most recent GAO, DHS OIG reports, or on the TSA.gov webpage. Keeping the above definitions in mind, it is apparent TSA's insider threat program relies on a variety of security programs focused primarily on employee/aviation worker background checks (vetting), physical security of personnel and facilities, and information technology system security. However, some of the tactics discussed in this section have a successful track record for detecting insider threats and

---

[84] Mark L. Reagan, ed., *Terms and Definitions of Interest for Counterintelligence Professionals* (Washington, DC: Department of Defense, 2014), 241.

[85] Ibid., 52.

[86] Mark L. Reagan, *Introduction to U.S. Counterintelligence-CI 101, a Primer* (Washington, DC: U.S. Department of Defense, 2005).

could be adopted by TSA to improve its ability to detect insider threats in the aviation system.

F. CHAPTER CONCLUSION

This chapter has discussed TSA's current policy for insider threat mitigation and the security programs used by TSA for this purpose. There have been some successes, but also some very troubling incidents involving insiders have occurred nonetheless. This chapter has also described several recent examples of insider threat cases and possible actors and that none of these individuals were identified as possible insider threats by TSA security programs. Clearly, identifying more aggressive measures could help TSA identify insider threats in the aviation system.

It is worth considering whether TSA should cross the threshold between security and CI and add a CI program to its current insider threat measures. In the words of arguably the most damaging American working as a spy for the Soviet Union, Robert Hanssen, "CI attacks the actor. It attacks the opposition intelligence structure. It is not speculative. CI feeds security because it helps them focus on meaningful measures and safeguards. Using CI to help security is just smart security."[87]

Chapter III discusses the insider threat policies and mitigation measures used by other entities that are responsible for addressing their own insider threat concerns. Some of these agencies, like the DHS I&A, have relatively new insider threat and CI programs. Others, such as the FBI, have robust programs and an established track record. The next chapter also looks at the policies used by the United Kingdom's MI5 as well as the program run by Lockheed Martin, a private defense contractor with substantial concerns for insider threat. Modeling and analyzing the insider threat programs of these entities can help identify a broad range of practices to help to determine what other measures TSA could consider implementing to improve its insider threat programs.

[87] Ibid., 11.

III. RAISING THE SHIELD (OR SWORD): HOW DO OTHER ORGANIZATIONS PROTECT THEMSELVES FROM INSIDER THREATS?

This chapter identifies and discusses the insider threat programs of four different organizations: DHS I&A, FBI, CPNI, and Lockheed Martin. These organizations represent a diverse mission set with significant concerns for insider threats. Exploring the practices of other organizations should inform us on the best recommendations to improve TSA's insider threat program.

A. DEPARTMENT OF HOMELAND SECURITY OFFICE OF INTELLIGENCE AND ANALYSIS

DHS I&A official mission is "to equip the Homeland Security Enterprise with the timely intelligence and information it needs to keep the Homeland safe, secure, and resilient."[88] I&A is tasked to ensure intelligence information from the 15 DHS component agencies is fused and analyzed to provide a common operational picture for the entire department.[89] DHS I&A has an interesting role within the DHS Intelligence Enterprise (IE) as both its own organization with Title 50 IC authority and the synergy point for the DHS IE. Part of this task includes the responsibility to coordinate intelligence analysis efforts across the six IE components within DHS that perform an intelligence mission. I&A is focused on five primary areas for intelligence production: border security, narcotics trafficking, alien and human smuggling, money laundering, and radicalization or extremism.[90]

Simultaneously, the head of I&A, also known as the DHS chief intelligence officer, serves as the primary connective tissue between DHS and the other federal agencies making up the IC. One of the chief intelligence officer's key responsibilities is

88 "Office of Intelligence and Analysis," U.S. Department of Homeland Security, last updated June 22, 2017, https://www.dhs.gov/office-intelligence-and-analysis.

89 Mark A. Randol, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress* (CRS Report No. 7–5700) (Washington, DC: Congressional Research Service, 2010).

90 Ibid.

to establish the intelligence collection, processing, analysis, and production priorities amongst members of the DHS IE.[91] In a sense, the DHS IE seeks to create the same intended synergy found among IC agencies but with focus on supporting the overall DHS and component agency missions. The former Secretary of Homeland Security, Michael Chertoff, also tasked I&A to be the primary source of intelligence information from the IC to state, local, and private sector partners.[92]

Title 50 is widely known as a portion of the U.S. Code containing multiple statutes relating to national security and foreign affairs. It is commonly used to grant intelligence collection and covert operations authorities to members of the IC. Of the six DHS IE components, only I&A and the U.S. Coast Guard are Title 50 agencies and are specifically identified as such in Title 50 U.S.C. § 3001.[93] This not only grants them authorities to collect information but also to protect the security and methods surrounding these collection activities (CI). This includes the ability to investigate the applicants, employees, and contractors associated with the IC as well as the physical protection of installations and the protection of virtual information.[94] Many of these activities are often considered part of an agency's CI mission in conjunction with an agency's security programs. Typically, CI collection within the United States is the responsibility of the FBI when targeting foreign intelligence elements. Other members of the IC are authorized to collect CI information concerning present and former employees or contractors only.[95]

Similar to TSA, DHS does not place all of its resources to counter insider threats into one office or function. The next section focuses on I&A's insider threat mitigation programs since DHS is moving towards expanding its CI program specifically for this effort. However, other security programs operated outside of I&A (but still within DHS)

---

[91] William E. Tarry Jr., *DHS Intelligence Enterprise* (Washington, DC: U.S. Department of Homeland Security, 2013).

[92] Randol, *The Department of Homeland Security*.

[93] War and National Defense, U.S.C. Title 50 § 3001 (2011), 434–435.

[94] Ibid., 435.

[95] Ibid.

will also be discussed as they play a significant role in the overall insider threat mitigation effort as well.

1. Scope and Current Policy

There are currently over 115,000 employees within I&A and the DHS component agencies that currently hold security clearances and positions that could be intelligence collection targets by adversary groups.[96] DHS defines insider threat as "the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States."[97] From the DHS purview, insiders who pose threats are capable of damaging the United States through "espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities."[98]

DHS operates its internal Insider Threat Program primarily designed to complement the department's CI and security missions.[99] DHS established the insider threat program after the issuance of Executive Order 13587 in 2011. Its goals are:

> To prevent the unauthorized disclosure of classified national security information, deter cleared employees from becoming insider threats, detect employees who pose a risk to classified national security information, and mitigate risks to the security of classified national security information through administrative, investigative, or other actions, while protecting the privacy, civil rights, and civil liberties of cleared personnel.[100]

The DHS chief security officer is responsible for the day-to-day management of the insider threat program, thus placing the operational control of the program outside DHS's CI Division.

---

[96] Taylor, Hayes, and McComb, *Counterintelligence and Insider Threats*, 6.

[97] U.S. Department of Homeland Security, *Privacy Impact Assessment for the DHS Insider Threat Program* (Washington, DC: U.S. Department of Homeland Security, 2015).

[98] Ibid., 1–2.

[99] Taylor, Hayes, and McComb, *Counterintelligence and Insider Threats*.

[100] U.S. Department of Homeland Security, *Privacy Impact Assessment*, 1.

In essence, the insider threat program protects against insider threats with security measures, such as information technology systems access controls and monitoring.[101] Its goals are indicative of DHS's concentration on identifying threats to classified information and data. To prevent unauthorized disclosure (witting and unwittingly), DHS collects and analyzes data about DHS employees[102] with security clearances, DHS stakeholders (public and private sectors) with security clearances, and others with a security clearance and access to DHS information technology systems or classified information.[103] DHS identifies possible insider threats by analyzing this data for indicators like unauthorized data transfers to mobile storage devices. Even more specifically, the insider threat program is designed to prevent unauthorized disclosure of classified information by collecting data from information technology system monitoring and tips from other cleared individuals (such as coworkers).[104]

Unique to DHS's insider threat program is its written emphasis on protecting the privacy, civil rights, and civil liberties of its employees.[105] For the legal authority to collect information on its employees and contractors, DHS cites multiple sources. For example, DHS cites both E.O. 12333 and Title 50 U.S.C. § 3381 (Coordination of CI Activities) as legal authorities for conducting this type of collection. This is where I&A's role becomes more prominent as the department's lead for CI activities.

The insider threat program is one leg of DHS's overall insider threat mitigation effort. According to 2016 testimony from the DHS chief intelligence officer, DHS also considers the insider threat issue as a subset of I&A's CI mission.[106] The overall I&A CI mission is to "prevent adversaries from penetrating the department to exploit sensitive

---

[101] Ibid., 6.

[102] DHS personnel refers to all personnel in DHS and all agencies under the department.

[103] DHS, *Privacy Impact Assessment*, 2.

[104] Ibid., 3.

[105] DHS is authorized to collect this information pursuant to the following: 1) Exec Order No. 13,587, CFR, (2011), 6; 2) White House, *National Insider Threat Policy*?; 3) U.S. Department of Homeland Security, *Information Sharing and Safeguarding* (DHS Directive 262–05), Rev 00 (Washington, DC: U.S. Department of Homeland Security, 2014); 4) U.S. Department of Homeland Security, *Insider Threat Program* (DHS Instruction 262–05-01) (Washington, DC: U.S. Department of Homeland Security, 2015).

[106] Taylor, Hayes, and McComb, *Counterintelligence and Insider Threats*, 7.

information, operations, programs, personnel, and resources."[107] One key goal is to integrate CI activities across the DHS IE so as to "deepen our understanding of the threats posed by foreign intelligence entities and insider threats to DHS."[108] Furthermore, the DHS I&A CI Division embeds officers in each DHS IE component to assist with CI functions and insider threat programs.

As part of this construct, DHS has created a CI and security board co-chaired by the DHS CI director (under I&A) and the DHS chief security officer to "integrate and align" CI and security programs across the various DHS agencies. The design of this board is meant to synchronize CI efforts with insider threat programs while combining the disciplines of CI and security to mitigate insider threats.[109] With this framework, DHS is using both an offensive (CI) and defensive (security programs) approach to mitigate insider threats.

2. Another Type of Insider Threat—Workplace Violence

In June of 2016, a non-supervisory I&A employee, Jonathan Wienke, was arrested while carrying a prohibited and concealed firearm inside of DHS headquarters. He was able to enter the building and proceed past the security checkpoint by taking advantage of his employee facility access and less security scrutiny due to his status as a vetted employee. Public court documents indicate he may have intended "to commit an act of workplace violence."[110] According to the court filing, the investigating agent discovered Wienke had a firearm along with several radios, thermal imaging devices, and a knife.[111] The agent also revealed there were reasons to believe Wienke intended to harm senior DHS officials meeting in the building that day.[112]

---

[107] Richard L. Skinner, *DHS Counterintelligence Activities* (Washington, DC: U.S. Department of Homeland Security, Office of the Inspector General, 2010), summary.

[108] Taylor, Hayes, and McComb, *Counterintelligence and Insider Threats*, 3.

[109] Ibid.

[110] Ibid.

[111] Scott MacFarlane, "Feds Investigating Whether Employee Was Plotting Attack on Homeland Security Officials," *News4 I-Team*, June 21, 2016, http://www.nbcwashington.com/investigations/Feds-Investigating-Whether-Employee-Was-Plotting-Attack-on-Homeland-Security-Officals-383852591.html.

[112] Ibid.

With Wienke, none of the DHS security programs involving background checks (vetting) identified him as an insider threat. The DHS insider threat program's focus is on detecting nefarious intent through information technology systems monitoring. Suspicious data acquisition or theft was not Wienke's intent, thus rendering this security program ineffective. In fact, Wienke was provided a Top Secret security clearance and was among one of the government's most vetted classes of employees.[113]

Herein lies one of the most critical challenges with the insider threat problem. In the case of I&A, using the department's definition that an insider threat is someone who uses their employee access to harm the United States, there are simply too many insider threat scenarios for a single security program to identify them all. Identifying a known terrorist or known felon attempting to join I&A can be accomplished during the initial vetting of new employees. However, absent indicators from a law enforcement investigation or targeted intelligence collection, it is very difficult to predict the intent of a Jonathan Wienke (or other vetted employees).

3. Final Thoughts on I&A's Insider Threat Program

The broader department (DHS) and I&A are newer government agencies lacking a lengthy historical record to analyze both previous insider threat cases and the success rate of its insider threat detection programs. At this point, it can be concluded that DHS's insider threat programs started off as predominantly security focused with detection measures primarily centered on employee vetting and network information technology system monitoring. In recent years, I&A has taken on a more aggressive role to detect and mitigate insider threats through its CI program and the leveraging of common IC authorities such as U.S.C. Title 50 and E.O. 12333. The ultimate goal of I&A's insider threat program is to integrate CI activities across the agencies comprising the DHS IE to better understand the threat from foreign intelligence entities and insider threats.[114] There is not enough data at this time to fully evaluate the effectiveness of I&A's CI program and insider threat mitigation.

---

[113] Ibid.

[114] Taylor, Hayes, and McComb, *Counterintelligence and Insider Threats*, 3.

The next section discusses the insider threat program of the FBI. The FBI has a defined track record and well established insider threat program along with some different authorities to investigate and collect domestic intelligence as both a law enforcement agency and an IC member.

B. FEDERAL BUREAU OF INVESTIGATION

Since its establishment in 1908, the FBI's mission and priorities have shifted over time to meet the most pressing law enforcement and domestic national security concerns of government.[115] Today, the official FBI mission statement is "To protect the American people and uphold the Constitution of the United States."[116] It prioritizes its mission sets by focusing on counterterrorism, counterintelligence, counterespionage, cybercrimes, public corruption, major white collar crime, protection of civil rights, and combatting transnational criminal organizations.[117] To accomplish this, it has over 56 field offices across the United States and an international presence at 60 U.S. embassies.[118] The FBI is a key component of the insider threat deterrence and investigation functions across the federal government and private sector.[119]

1. Scope and Current Policy

The FBI's insider threat concern is essentially twofold. First, it has over 35,000 employees,[120] illustrating the magnitude of the insider threat potential within its ranks. Second, per U.S.C. Title 50, it is the lead agency for domestic intelligence collection concerning foreign intelligence entities and CI, "including such information concerning corporations or other commercial organizations."[121] The FBI's insider threat program is

115 "Mission and Priorities," Federal Bureau of Investigation, accessed October 15, 2017, https://www.fbi.gov/about/mission.

116 Ibid.

117 Ibid.

118 Ibid.

119 Ibid.

120 Ibid.

121 War and National Defense, U.S.C. Title 50 § 3001 (2011), 435.

primarily managed under the purview of its CI Division.[122] However, security standards similar to those conducted by other U.S. government law enforcement and intelligence agencies are in place to vet employees prior to and during employment with the FBI. An FBI background investigation for Top Secret security clearance is required.[123] This is then followed by "a polygraph examination; a test for illegal drug use; credit and records checks; and extensive interviews with former and current colleagues, neighbors, friends, professors, etc."[124] Today, the FBI performs a recurrent background investigation every five years and often along with another polygraph.[125]

The FBI's insider threat program also has a CI component and focus to it, and this relates directly to its traditional role mitigating national security threats from foreign intelligence entities. Thus, the FBI's CI Division is "the lead agency for exposing, preventing, and investigation of intelligence activities on U.S. soil, and the Counterintelligence Division uses its full suite of investigative and intelligence capabilities to combat counterintelligence threats."[126] This traditional CI mission also applies directly to insider threat investigations. According to the FBI website, addressing insider threats relates to three of its four strategic goals:

1. Protect the secrets of the U.S. Intelligence Community, using intelligence to focus investigative efforts, and collaborating with our government partners to reduce the risk of espionage and insider threats.
2. Protect the nation's critical assets, like our advanced technologies and sensitive information in the defense, intelligence, economic, financial, public health, and science and technology sectors.
3. Counter the activities of foreign spies. Through proactive investigations, the Bureau identifies who they are and stops what they're doing.

---

[122] "What We Investigate-Counterintelligence," Federal Bureau of Investigation, accessed October 15, 2017, https://www.fbi.gov/investigate.

[123] "FBI Jobs," Federal Bureau of Investigation, accessed September 19, 2017, https://www.fbijobs.gov/working-at-FBI/eligibility.

[124] Ibid.

[125] Glenn A. Fine, *A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen* (Washington, DC: U.S. Department of Justice, 2003), 22.

[126] "What We Investigate-Counterintelligence," Federal Bureau of Investigation.

4. Keep weapons of mass destruction from falling into the wrong hands and use intelligence to drive the FBI's investigative efforts to keep threats from becoming reality.[127]

The first goal explicitly ties espionage with insider threats. Indeed, insiders are commonly used to conduct espionage on behalf of a foreign intelligence entity or service. In Department of Defense circles, this is known as the "CI insider threat," insiders who pose threats using their legitimate employee access to commit espionage on behalf of a foreign intelligence entity.[128] This can be the case whether at a government agency or a private defense contractor. Goals two and three go hand in hand as they identify our nation's critical assets and the need to protect these assets from the activities of foreign spies.

The FBI CI Division utilizes a myriad of private sector and higher education engagement programs to help deter and investigate insider threats. Similar to the approach by CPNI (as discussed in the next subchapter), the FBI also conducts outreach to organizations in the private sector and academia to assist them with identifying personal factors, organizational factors, and behavioral indicators that could point toward a possible insider threat. The FBI has openly published less details on what its "profile" is for an insider threat, but it hints that lax security measures and enforcement along with a perfect storm of personal factors could make an employee more susceptible to recruitment by a foreign intelligence service or terrorist organization.[129]

The FBI is particularly active in private sector outreach to help prevent economic espionage from insider threats. According to its website, "(f)oreign economic espionage against the U.S. is a significant and growing threat to our country's economic health and security...and so is the threat from corporate insiders willing to carry it out."[130] The basic message is clear: American companies are choice targets for foreign intelligence entities,

---

[127] Ibid.

[128] Michael J. Vickers, *Department of Defense Instruction: Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat* (Washington, DC: U.S. Department of Defense, 2012), https://www.hsdl.org/?view&did=745624, 13.

[129] Federal Bureau of Investigation, *The Insider Threat.*

[130] "Economic Espionage: How to Spot a Possible Insider Threat," Federal Bureau of Investigation, May 11, 2012, https://www.fbi.gov/news/stories/how-to-spot-a-possible-insider-threat.

criminals, and industry spies. A common method for stealing proprietary industry information is through insiders working at these companies. The FBI believes insiders often exhibit signs and indicators of their intent to act nefariously, but the signs are missed by co-workers.[131] The FBI focuses its outreach efforts on educating private industry on what these indicators are and what types of economic information insider threats are most likely to target them.[132]

The FBI runs a private sector outreach program called the FBI Business Alliance Initiative. The goal of this program is a "partnership effort between the FBI and private industry to protect research, products, and personnel from foreign intelligence threats."[133] This program specifically identifies the insider threats as persons that have been recruited by foreign intelligence services or terrorist organizations.[134] Thus, much of the program's focus is on CI education in order to protect trade secrets and prevent economic espionage while encouraging suspicious incident reporting from the private industry stakeholder to the FBI.[135] The FBI claims this initiative has assisted the private sector by increasing its knowledge and understanding of threats. The FBI also claims it has reciprocally received much broader awareness of private sector issues and concerns, as well as investigative leads.[136]

Another key component of the FBI's overall insider threat deterrence effort with the private sector is in the creation of multi-disciplinary threat assessment teams. These teams use behavioral indicators that the FBI identifies as possible signs of insider intent. Indicators could be personal workplace grievances, new interest in explosives or firearms, and fascination with other active shooter events in the media.[137] Threat assessment teams are recommended to contain members of management, security

[131] Ibid.

[132] Ibid.

[133] "The FBI Business Alliance Initiative" Federal Bureau of Investigation, accessed October 15, 2016, https://www.fbi.gov/file-repository/us-business-alliance-brochure.pdf.

[134] Ibid.

[135] Ibid.

[136] Ibid.

[137] Ibid.

personnel, counselors, mental health professionals, and other company employees. Threat assessment teams would then be ideally trained and ready to identify possible signs of insider threat intent and hopefully deter or interdict the threat before the insider can act. Threat assessment teams are also ready to interface with law enforcement and the FBI if needed for assistance.[138]

The FBI also plays a key role in the overall organizational construct across the U.S. government to deter insider threats. Together with the National Counterintelligence Executive (from the Office of the Director of National Intelligence), the FBI co-chairs the National Insider Threat Task Force which operates under the purview of the NCSC.[139] The NCSC works under the Office of the Director of National Intelligence (ODNI) and provides expertise to executive department agencies and the private sector on insider threats, personnel security, and supply chain risk management.[140] This organizational hierarchy reaffirms the connection between security and CI and the shared mission to combat insider threats.[141] Unlike TSA, the FBI uses both the security and CI disciplines to counter insider threats.

The FBI is actively engaged in insider threat investigation within the aviation system as well. In a 2015 statement to the House Committee on Homeland Security Subcommittee on Transportation Security, the deputy assistant director of the FBI's Counterterrorism Division described the FBI's efforts to work closely with all stakeholders in the aviation system (public and private).[142] One of the major efforts he described is the FBI's Civil Aviation Security Program. This program falls under the

---

138 "Spotting Insider Threats" (Federal Bureau of Investigation, Office of Private Sector, accessed October 15, 2016, https://www.fbi.gov/file-repository/spotting-insider-threat_508.pdf.

139 National Counterintelligence and Security Center [NCSC], *National Insider Threat Task Force Mission Fact Sheet* (Washington, DC: National Counterintelligence and Security Center, https://www.dni.gov/files/NCSC/documents/products/National_Insider_Threat_Task_Force_Fact_Sheet.pdf.

140 "How We Work," NCSC.

141 Ibid.

142 *FBI's Role in Access Control Measures at Our Nation's Airports, House Committee on Homeland Security, Subcommittee on Transportation Security* (2015), (statement of Doug Perdue, Deputy Assistant Director, Counterterrorism Division), https://www.fbi.gov/news/testimony/fbis-role-in-access-control-measures-at-our-nations-airports, 3.

authority of the FBI Counterterrorism Division and assigns airport liaison agents to each U.S. federalized airport. The liaison agents partners with TSA to perform vulnerability assessments and interact with private stakeholders in the aviation system.[143] Finally, the program has produced intelligence products for the IC designed to mitigate the insider threat in the aviation system.[144]

2. When All Fails: The Case of Robert Hanssen

Despite the FBI's aggressive efforts and domestic CI authorities, the agency has experienced its own insider threat problems. On July 6, 2001, Robert Hanssen pled guilty to 15 counts of espionage and conspiracy over a 20 year period.[145] During this period, he sold secrets to the Soviet Union and Russia for $1.4 million in cash and diamonds.[146] He is considered by many analysts to be the most damaging spy in U.S. history and the impact caused by his espionage has been described by the FBI as "exceptionally grave."[147] Hanssen's case illustrates the concern of foreign intelligence entity insider threats. This threat stems from a foreign intelligence or government agency recruiting and handling an insider threat for the purpose of stealing information the insider has legitimate employee access to.[148]

Hanssen began his espionage a few years into his career and continued off and on until February 2001 (when he was arrested). He was assigned to multiple assignments at FBI headquarters and even the State Department (as an FBI employee), and he was also granted access to highly sensitive CI and military information. Moreover, he compromised significant secrets, including the identities of human sources in the Soviet Union, which led to the execution of at least three of them. In addition, he provided the

---

[143] Ibid.

[144] Ibid.

[145] Fine, *A Review of the FBI's Performance*, 2.

[146] "Ex-FBI Spy Hanssen Sentenced to Life, Apologizes," *CNN*, May 14, 2002, http://www.cnn.com/2002/LAW/05/10/hanssen.sentenced/index.html?_s=PM:LAW.

[147] Ibid.

[148] Office of the Director of National Intelligence, *Countering Foreign Intelligence Threats: Implementation and Best Practices Guide* (Washington, DC: Office of the Director of National Intelligence, 2017), https://www.dni.gov/files/NCSC/documents/campaign/Guid_CFIT-Implementation-and-Best-Practices-Guide_2017-06-08_UNCLASS_LINKED.pdf.

KGB thousands of pages and dozens of computer disks "detailing U.S. strategies in the event of nuclear war, major developments in military weapons technologies, information on active espionage cases, and many other aspects of the U.S. IC's Soviet CI program."[149]

Interestingly, Hanssen's day-to-day behavior did not suggest he was involved in espionage, nor did it match many of the common signs of insider threat as exhibited by employees who pose an insider threat. His personal life did not fit a profile consistent with that of a spy. According to Fine, "He was married with six children, and appeared to be a devout Catholic…had no alcohol, drug, or gambling problems and did not engage in ostentatious spending."[150] However, he did display some financial habits that were possible indicators as well as a general inability and unwillingness to properly handle classified information. Nonetheless, these factors were largely ignored and undocumented, which allowed Hanssen to continue his espionage activities.[151] Important to note is the FBI's initial vetting (background investigation), pre-employment interviews, and periodic reviews of his suitability for continued access to sensitive information did not specify that Hanssen was expected to commit espionage.[152] It only became apparent after he was caught that he suffered from "serious personal insecurities, low self-esteem, and a fascination with espionage."[153] His pattern of mishandling classified information began early in his career, but this was not solely pertaining to his espionage activities. For example, he became known for disclosing the existence of Soviet sources to people without a "need to know," such as other FBI employees in other divisions. Additionally, there was an instance in which he committed a serious security violation when he disclosed sensitive information to a Soviet defector he was debriefing.[154]

---

[149] Fine, *A Review of the FBI's Performance*, 2.

[150] Ibid., 5.

[151] Ibid., 2.

[152] Ibid., 5.

[153] Ibid.

[154] Ibid., 7.

While Hanssen was a liaison for the FBI at the State Department, he committed multiple security violations as well. He disclosed classified information to other agencies and employees (without a need to know), to close friends, and members of the press. At one point, he even attempted to install a password breaker program on his FBI computer. Although the last incident was detected and referred to the FBI's security programs manager, Hanssen was able to adequately excuse his behavior and thus avoid any negative consequences for his actions.[155] Systemic failures to document, report and take seriously so many security violations represent both a serious management failure and an organizational culture failure over two decades that repeatedly ignored concerning behaviors.

3. Conclusion—A Shift toward "Trust, but Verify"

The case of Robert Hanssen uncovered an overall lack of organizational controls and a workplace culture that enabled multiple instances of espionage and the inappropriate revelation of classified materials to be overlooked. Even worse, with 20/20 hindsight, it is clear the FBI not only ignored Hanssen's repeat security violations but also continued to promote him into positions with less supervisory oversight and access to more sensitive classified information. However, the Hanssen case did lead to a cultural shift and a "tightening down" of the security programs and on the workplace culture that had enabled his 20-plus years of espionage to occur. Instead of an insider threat program, which assumes a blanket level of trust in each employee, the FBI now requires verification via polygraphs, computer usage monitoring, financial disclosures, and periodic background reinvestigations, among other measures.[156]

When compared to TSA, the FBI can leverage its additional law enforcement and CI authorities to further detect and investigate insider threats. Many of the security programs used by both agencies are similar, such as background checks (security clearances) and information technology systems monitoring. The FBI does appear to now require additional security precautions, such as financial disclosure forms and employee

[155] Ibid., 9.

[156] Ibid., 21.

polygraphs, which TSA does not generally require. Both agencies also work with external stakeholders and private sector companies to advise them on the seriousness of the insider threat. The key difference is that if TSA identifies suspicious behaviors indicative of a possible insider threat, it typically refers any follow up investigation to another agency, such as the FBI. The FBI is able to receive both internal and external referrals and proceed with either a CI collection operation or law enforcement investigation as needed.

The following section takes us across the Atlantic Ocean to the United Kingdom to compare the insider threat policy from the English perspective. For the purpose of exploring a wide range of policy options, it is worthwhile to consider a foreign government agency with an established track record dealing with the insider threat problem.

C. UNITED KINGDOM: CENTRE FOR PROTECTION OF NATIONAL INFRASTRUCTURE

The United Kingdom United Kingdom executes insider threat mitigation policy though CPNI, which reports to the director general of MI5. CPNI takes on the role of expert advisor to both the government and private sector entities comprising the United Kingdom's national critical infrastructure.[157] This agency is an excellent example to examine because MI5 combines CI, counterterrorism, national security, and national level intelligence and investigation functions into a single agency. In comparison to the U.S. government, these functions are generally spread out across various agencies although the FBI's mission and range of authorities shares some commonality with MI5. By "housing" all these functions at the national level within a single agency, we can establish a good comparison architecture for TSA and consider how an entity with broad investigation and intelligence collection authority counters insider threats. Like TSA, CPNI is also a relatively new organization, created on February 1, 2007 out of the merger

[157] "About CPNI," Centre for the Protection of National Infrastructure.

of the former National Infrastructure Security Co-ordination Centre and the National Security Advice Centre.[158]

CPNI's primary function is to protect the United Kingdom's national infrastructure. This lines up nicely with its parent organization's (MI5) mission statement. Simply stated, "MI5's mission is to keep the country safe."[159] In addition to insider threat prevention through the purview of CPNI, MI5 is responsible for

> the protection of national security and in particular its protection against threats such as terrorism, espionage and sabotage, the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.[160]

These functions align with many aspects of the CI mission in the United States and the insider threat is a problem within each of these areas. This is important to point out because the policy development and outreach efforts of CPNI can result in direct internal referrals to the investigatory and intelligence collection branches of MI5. In this manner, TSA and CPNI are very similar. TSA lacks a true law enforcement investigation and intelligence collection capability and therefore generally refers insider threat issues to another federal agency, such as the FBI, with law enforcement authority. From a review of some of the more substantial insider threat cases discussed in Chapter II, it is reasonable to conclude the majority of TSA's insider threat cases are referred to the FBI for investigation.

1. Scope and Current Policy

The United Kingdom government breaks its critical national infrastructure into nine different sections: communications, emergency services, energy, finance, food, government, health, transport, and water.[161] For the sake of comparison, these sectors

---

158 "Centre for the Protection of National Infrastructure," *Wikipedia*, accessed June 8, 2017, https://en.wikipedia.org/wiki/Centre_for_the_Protection_of_National_Infrastructure.

159 "Security Service MI5," Security Service MI5, accessed April 29, 2017, https://www.mi5.gov.uk/.

160 "What We Do," Security Service MI5, accessed April 29, 2017, https://www.mi5.gov.uk/what-we-do.

161 "Critical National Infrastructure," Center for the Protection of National Infrastructure, 2017. https://www.cpni.gov.uk/critical-national-infrastructure-0.

generally overlap with DHS's critical infrastructure sectors in the United States.[162] Within these sectors lies a potential threat from terrorism, espionage, sabotage, and the activities of agents of foreign powers. CPNI "provides security guidance, training, and research from a physical, information and personnel security perspective. It aims specifically to reduce vulnerabilities within these sectors…"[163] When it comes to insider threats, CPNI focuses on persons who exploit or have "the intention to exploit, their legitimate access to an organization's assets for unauthorized purposes."[164] It is within this purview that CPNI oversees and advises the national infrastructure on insider threat issues and their mitigation.

CPNI is a consumer of the United Kingdom's national threat intelligence and uses this information to provide guidance to its national infrastructure operators to help them understand the threats it faces.[165] Its focus is on prevention through awareness and it utilizes behavioral factors and models as information to help an organization create a culture of security.[166] An area of primary emphasis is its focus on management's role in creating an environment that minimizes insider threat vulnerabilities.[167] However, perhaps most important is CPNI's recognition of the need for private sector engagement within the United Kingdom's critical infrastructure.[168] According to the government of the United Kingdom , the vast majority of these services are owned by the private sector. Other estimates indicate as much as 85 percent of national critical infrastructure facilities

---

[162] "Critical Infrastructure Sensors," U.S. Department of Homeland Security, last updated July 11, 2017, https://www.dhs.gov/critical-infrastructure-sectors.

[163] Center for the Protection of National Infrastructure [CPNI], *Investigating Employees of Concern: A Good Practice Guide* (London: Center for the Protection of National Infrastructure, 2011), 2.

[164] CPNI, *CPNI Insider Data Collection*, 4.

[165] "What We Do," Security Service MI5.

[166] Center for the Protection of National Infrastructure [CPNI], *Personnel Security: An Ongoing Responsibility-Understanding Insider Threats-and Minimizing the Risk* (London: Center for the Protection of National Infrastructure, 2015), https://www.cpni.gov.uk/system/files/documents/5b/04/ongoing-personnel-security-infographic.pdf.

[167] CPNI, *Investigating Employees of Concern*.

[168] "About CPNI," CPNI.

are privately owned.[169] With such a large portion of the United Kingdom's critical infrastructure owned by the private sector, it is crucial from a national security standpoint to engage and share information with these stakeholders.

According to CPNI, there are five main types of insider activity: "unauthorized disclosure of sensitive information; process corruption; facilitation of third party access to an organization's assets, physical sabotage; and electronic or IT sabotage."[170] CPNI strictly maintains an advisory and assessment role, and it does not directly collect intelligence or investigate suspicious activity. CPNI recommends organizations contact law enforcement to address illegal activity. However, if an employer believes an employee has a tie to terrorism or extremism, CPNI prefers to initially handle the investigation and refer it internally within MI5 as needed. When called upon, CPNI examines the information and may pass the information on to relevant investigatory bodies for follow up.[171]

CPNI favors using insider threat risk assessment models to help an organization realize the security vulnerabilities an insider posing a threat might try to compromise. Its models focus on the following elements:

1. Identify the critical assets
2. Identify the threat based on intent and capability of the insider
3. Assess the likelihood of the threat occurring
4. Assess the business impact if the threat occurred
5. Review and evaluate effectiveness of existing countermeasures
6. Propose new appropriate measures to reduce security risks.[172]

Once CPNI identifies risks, these are then used to create implementable security procedures designed to mitigate insider threats. CPNI provides an extensive risk

[169] Warrick Ashford, "Is UK Critical National Infrastructure Properly Protected?," *Computer Weekly*, March 3, 2011, http://www.computerweekly.com/news/1280097313/Is-UK-critical-national-infrastructure-properly-protected.

[170] CPNI, *CPNI Insider Data Collection*, 4.

[171] CPNI, *Investigating Employees of Concern*, 29.

[172] "Insider Risk Assessment," Centre for the Protection of National Infrastructure, accessed October 29, 2017, https://www.cpni.gov.uk/insider-risk-assessment.

assessment model focusing on the job roles of employees, their access within the organization's critical assets, and the risk their positions pose to the organization if an insider threat is present.[173] The CPNI risk assessment models focus on the organizational structures, policies, and vulnerabilities to an insider threat. By completing the assessments, an organization will have more clarity regarding the likelihood an insider threat is present, the areas targeted by the insider, and the most appropriate mitigation measures to reduce vulnerabilities.

CPNI also conducts detailed studies of the profile and behavioral indicators of a possible insider threat by a perpetrator based on data from previous insider threat cases. Although they are still applicable, CPNI's data indicates the effectiveness of pre-employment checks as a preventative measure is perhaps overstated. From its research into insider threat cases in the United Kingdom, CPNI has identified that 76 percent of perpetrators did not join their organization intending to commit an insider act.[174] It is sometime after their initial employment when they decide to leverage their position and employee access to carry out an insider threat.[175] In fact, CPNI found that only six percent of insider threat cases in its study involved a perpetrator who sought employment specifically to further an insider plot.[176] This is particularly concerning given the focus TSA places on pre-employment background checks and vetting to prevent insider threats, which this data would indicate is not effective on its own. In comparison, TSA continues to emphasize aviation worker vetting (initial and recurrent) as a primary tactic for preventing insider threats from being employed in the aviation system.

Another facet of CPNI's outreach efforts is designed to highlight organizational deficiencies with the potential of leading to more exploitable weaknesses within an organization's security and management practices. CPNI identifies several organizational traits it believes are key enablers for insider acts. They are

---

[173] "Reducing Insider Risk," Center for the Protection of National Infrastructure, accessed 17 November, 2017, https://www.cpni.gov.uk/reducing-insider-risk.

[174] CPNI, *CPNI Insider Data Collection*, 9.

[175] CPNI, *Personnel Security*.

[176] CPNI, *CPNI Insider Data Collection*, 9.

1. Poor management practices
2. Poor usage of auditing functions
3. Lack of protective security controls
4. Poor security culture
5. Lack of adequate role-based personnel security risk assessment prior to employment
6. Poor pre-employment screening
7. Poor communication between business areas
8. Lack of awareness of people risk at a senior level and inadequate governance.[177]

This list of exploitable organizational weaknesses identifies many factors that TSA does not appear to consider. TSA's focus is on pre-employment screening (vetting), suspicious indicators (once employed), and physical access control. In contrast, CPNI places a lot of effort on identifying management's role in establishing a workplace environment and culture to decrease insider threat vulnerabilities. Most failures in organizational practice are management failures to establish proper policies and a proper security culture for mitigating insider threats.

One of the main initiatives created and executed by CPNI is known as the Motivation Project. This is an interactive survey designed to achieve a highly inspired security workforce within the United Kingdom's critical infrastructure facilities. It seeks to create the conditions in which "a highly motivated workforce can have a beneficial impact on performance, attitudes and behaviours, and support … business efficiency and effectiveness."[178] The practical guidance suggests that high workforce drive leads to more efficient security. CPNI's approach is to encompass all the factors identified above regarding insider threat indicators and to create a high performing security culture limiting insider threat vulnerabilities through awareness and proactive reporting. The Motivation Project is representative of a holistic approach to organizational culture and

[177] Ibid.

[178] Centre for the Protection of National Infrastructure, *Motivation within the Security Industry* (London: Centre for the Protection of National Infrastructure), https://www.cpni.gov.uk/.../documents/52/73/guard-force-motivation.pdf.

management to naturally deter insider threats due in large part to high levels of workforce drive to create a high performing security organization.[179]

The critical factor measured by the Motivation Project is not just the level of motivation within the security workforce, but the *type* of motivation as well. A staff that is highly driven but misdirects its enthusiasm can be problematic. For example, employees might be highly ambitious and capable but management's expectations of them are too low, which creates a culture of low performance. On the other hand, the company's culture can be so poor it actually creates high levels of incentive for employees to behave in counterproductive ways. CPNI believes insider threats are the direct byproduct of a negative management security culture that opens itself up to the eight organizational practices identified above that are considered to be key enablers.[180] TSA does not appear to consider these points, and its focus on vetting and access control suggests TSA believes insider threat perpetrators are uniquely susceptible (or even pre-determined) to becoming insider threats from day one.

2. Organizational Culture as Insider Threat Mitigation

In a 2011 case study involving the Motivation Project, CPNI worked with Birmingham Airport in the United Kingdom to introduce positive efficiency changes by improving workplace motivation. Birmingham Airport is an interesting example because it represents one of the United Kingdom's busiest airports while simultaneously experiencing rapid growth and changes to its infrastructure. Birmingham Airport employs over 200 security staff for security screening checkpoint operations. In recent years, it has seen substantial operating changes through a redesign of the checkpoint environment and the introduction of new technologies and systems.[181]

The CPNI motivation survey identified four key areas for improving staff motivation: performance feedback, team building, job fundamentals (breaks and rotations), and management fairness and consistency. CPNI's survey results helped

[179] Ibid., 1.

[180] Ibid.

[181] Ibid.

Birmingham Airport to come up with a set of short-, mid-, and long-term initiatives for its employees. The first step was to pull the top layer of management from the frontline operations. In turn, this enabled greater flexibility and operational control for the frontline managers, and they became the only management level in direct contact with frontline employees.

Step two changed the job title of the rank and file from "guard" to "security duty officer."[182] This step was designed to change the culture from one guarding a specific area to that of an "officer" who "delivers a great security service coupled with great customer service."[183] The change in job title also served to further professionalize the position and duties.

The third step was to adapt a different approach to customer service to train all officers to better communicate with the differing personalities of the public they serve. Step four was to improve supervisor performance by measuring employees in new areas such as customer service, cost efficiency and compliance. The fifth step similarly improved supervisor performance by requiring a monthly one-on-one sit down with each employee to increase trust and confidence within this relationship. Finally, came the establishment of several workplace improvements and mentorship/employee growth opportunities to improve communication and staff development.[184]

The initial product of these changes was a significant improvement and greater unity as a team. Leaders developed a keener sense of purpose and trust with their subordinates improved substantially.[185] The Birmingham Airport example is a good case study of a successful implementation of CPNI's private sector insider threat mitigation engagement strategy because it directly addresses the eight organizational practices identified in the previous section that are key enablers for insider threats. The motivation survey and outreach are enviable as is its understanding of the enterprise perspective of cultural factors that "create" insider threats due to employee job dissatisfaction. The

[182] Ibid.

[183] Ibid.

[184] Ibid.

[185] Ibid.

Birmingham Airport example shows that perhaps the best byproduct of increasing security force motivation is the creation of a proactive security culture to minimize the organization's vulnerable points to an insider threat.

3. Conclusion—Proactive Prevention through Organizational Culture

CPNI places a heavy emphasis on identifying and detecting the root causes of an insider threat from the perspective of the perpetrator, management culture, and the victimized organization. With this mindset, CPNI preaches a message of proactive prevention through organizational culture as the best policy for mitigating insider threats. This starkly contrasts with the U.S. government's approach, which focuses on the integration of security, CI, user audits/monitoring, and "other safeguarding capabilities."[186] CPNI considers such practices as part of an overall insider threat policy, but it attempts to do more on the front end with its management culture and workplace environment to minimize enablers and vulnerabilities. TSA's emphasis is on identifying known risks during the vetting process and physical access control procedures. Like CPNI, TSA has an outreach responsibility to external stakeholders in the aviation domain such as airport operators and airlines and is ideally positioned to receive suspicious activity reports pointing to possible insider threat activity.

TSA can also provide referrals to other investigating organizations when external stakeholders report suspicious activity to TSA. So there are some similarities in insider threat mitigation efforts between CPNI and TSA. However, there are two major differences to consider. First, TSA does not have an investigation or a CI mission and must reach out to external agencies to further develop an insider threat investigation. As part of MI5, CPNI can refer suspicious indicators reported by the private sector to its internal investigations and domestic intelligence collection teams. Second, TSA does not consider organizational culture and management policies and practices as key enablers to insider threat vulnerabilities as CPNI does.

The last section of this chapter introduces the insider threat program operated by a private company and major defense contractor, Lockheed Martin. This company has a

[186] White House, *National Insider Threat Policy*?

history of addressing insider threats (mainly from the foreign espionage angle) and a very mature program worth evaluating.

D. LOCKHEED MARTIN

Lockheed Martin is a "global security and aerospace company that employs approximately 97,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services."[187] Its overall mission is to "solve complex challenges, advance scientific discovery and deliver innovative solutions to help our customers keep people safe."[188] Its business is divided into four separate operating units: aeronautics, missiles and fire control, rotary systems, and space systems.[189] In plain language, Lockheed Martin builds high tech aircraft, missiles, missile defense systems, helicopters, and satellites (including delivery vehicles) along with all of the research, logistics, and operations required to create and produce these systems.

Lockheed Martin's primary customer base is the U.S. Department of Defense and other federal government agencies. It also has a large international presence in at least 70 countries and over 7,000 international employees.[190] Its future investments are primarily in the development of advanced weapon and protection systems involving robotics, direct energy weapons, electronic warfare, and cyber security.[191] Additionally, Lockheed Martin develops and produces cutting edge, sensitive technologies primarily for battlefield usage. As a result, the company must consider the consequences of having its technology and research compromised by an insider working, whether intentionally or unwittingly, for a foreign intelligence entity and posing a threat to the company. In fact,

---

[187] "Who We Are," Lockheed Martin, accessed April 29, 2017, http://www.lockheedmartin.com/us/who-we-are.html.

[188] Ibid.

[189] Ibid.

[190] "Lockheed Martin Fact Sheet," Lockheed Martin, 2016, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/lockheed-martin-fact-sheet.pdf.

[191] Ibid.

Lockheed Martin directly correlates its international presence with increased exposure to foreign intelligence entities, in turn leading to an increase in insider threats.[192]

1. Scope and Current Policy

Lockheed Martin's immediate insider threat concern starts from within the company's 97,000 employees. However, the company recognizes that it must consider its contractors, suppliers, and other business partners that have authorized access to the company's systems and information as possible sources of insider threats as well.[193] The company's large international presence offers additional exposure opportunities to foreign intelligence entities that TSA generally does not experience, certainly not to the same scale. The company's Director of Counterintelligence Operations and Corporate Investigations, Douglas Thomas, is also concerned that periods of global economic downturn could lead to increased foreign intelligence entity attempts to acquire new technologies and research, resulting in increased attempts to steal industry information from American firms overseas.[194] According to Robert Trono, Vice President and Chief Security Officer at Lockheed Martin, "U.S. corporations have seen a dramatic increase in economic and industrial espionage threats over the past five years, and we do not see this trending data decreasing for the foreseeable future."[195] It is thus reasonable to conclude that Lockheed Martin is very aware of the threat posed by a foreign intelligence entity using a company insider to steal proprietary technology for both economic and military benefits.

---

[192] Douglas D. Thomas, "Lockheed Martin Counterintelligence and Insider Threat Programs" (presented at Annual Industry Security Conference, Washington, DC, 2015), http://www.connectidexpo.com/creo_files/2015_day1/16.15%20Douglas%20D.%20Thomas%2023%20Mar%202015%20Connect%20ID%20Expo.pdf, 6.

[193] Lockheed Martin, *5 Steps to Develop a Successful Insider Threat Detection Program* (Bethesda, MD: Lockheed Martin, 2015), http://informationsecurity.report/Resources/Whitepapers/2e8a0821-6982-4666-8e46-bd7153a6989f_5%20Steps%20to%20Develop%20a%20Successful%20Insider%20Threat%20Detection%20Program.pdf, 2.

[194] Thomas, "Lockheed Martin Counterintelligence."

[195] "Lockheed Martin Insider Threat Detection Program Recognized by CSO Magazine for Defining Future of Security," Lockheed Martin, January 2014, http://www.lockheedmartin.com/us/news/press-releases/2014/january/01142014-isgs-insider-threat-detection-cso.html.

Lockheed Martin has a well-established and proactive insider threat program. The company is generally recognized as an industry leader in insider threat mitigation and was selected in 2014 by *Chief Security Officer (CSO) Magazine* as one of the top 40 companies that demonstrate outstanding business value and thought leadership for security project initiatives.[196] In particular, the company was lauded for its Insider Threat Detection Program (ITDP) as it

> proactively identifies and mitigates internal risks associated with the theft or misuse of intellectual property and trade secrets. It can identify employees who are at higher risk for being targeted by foreign intelligence or those who are more likely to misuse access privileges to protected information.[197]

The ITDP has also been praised within the U.S. government and among companies in the private sector as the "model" program, according to Robert Trono.[198] Based on its requirements as a defense contractor working on classified technology, many employees must undergo security clearance (background) investigations and must revalidate their security clearances annually.[199]

The Lockheed Martin ITDP defines the following five steps as the vital components of its ITDP:

1. Gain leadership support
2. Leverage the latest technology
3. Develop a communications plan
4. Execute a training and awareness campaign
5. Establish a governance structure[200]

The first step requires attaining support across the executive leadership team not just in principle, but to the point at which leaders fully understand the types of threats

---

[196] Ibid.

[197] Ibid.

[198] Ibid.

[199] Lockheed Martin, *Counterintelligence Awareness: Capability Without Compromise* (Bethesda, MD: Lockheed Martin, 2015), https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/clearanceconnection/CI_Awareness_briefing.pdf.

[200] Lockheed Martin, *5 Steps to Develop*, 3.

facing the company and the consequences if the company falls victim to those threats. Within this step is demonstration to employees that the ITDP is aligned with the company's culture, and it addresses both privacy and legal concerns.[201] This is a point worth expanding upon from a comparison standpoint with TSA. Although it is reasonably implied that TSA's insider threat programs have leadership support (or the programs likely would not exist), a big difference in Lockheed Martin's approach is that it formalizes this step and takes additional steps to ensure leadership buy in across the company's various organizational layers. Another side effect of leadership buy in is assistance in gathering financial support for insider threat initiatives. This is a critical component given the need for more and more advanced information technology and digital monitoring systems to detect insiders attempting to steal data from the company's information technology systems.[202]

Second, the ITDP leverages technology as a key component. This goes beyond just cyber, data loss, and information technology monitoring capabilities and also feeds into an analytical tool to make the data useable to a CI investigator. In essence, this enables identifying what the company refers to as "anomalous behavior" on its networks that cues an internal CI inquiry.[203] These analytical tools are designed to integrate with "network and behavioral risk indicators from other business functions such as HR and corporate security."[204] The purpose is to provide proactive prioritization for follow up investigations on those portraying behavioral risk indicators both in their daily interactions with other employees and their information technology system usage. Thus, the latest technology solution can utilize big data to provide the most accurate investigatory leads and better analysis of behavior on company systems of an insider who poses a threat.[205]

---

[201] Ibid.

[202] Ibid.

[203] Emily Kopp, "How Lockheed Martin Sold Employees on an Insider Threat Program," *Federal News Radio*, October 30, 2015, https://federalnewsradio.com/defense-industry/2015/10/lockheed-martin-sold-employees-insider-threat-program/. program/.

[204] Ibid., 3.

[205] Ibid.

Step three of the ITDP is establishing a companywide communications plan and strategy before new insider threat policies and protocols are initiated. Lockheed Martin regards this step as "opaque transparency," and it is designed to gain support and close coordination with multiple departments while not giving away the critical components of the program.[206] One of the interesting things Lockheed Martin discovered in this stage is the benefit of receiving feedback from the company rank and file on the message before it is pushed out to all employees. For example, inflammatory or counterproductive language interpreted as fostering a "big brother" or "snitch" mentality can be eliminated to help garner employee and management support.[207]

Next, Lockheed Martin established a training and awareness campaign (step four) to not just educate it employees on the insider threat issue but also to alleviate employee concerns. It trains on internal and external threats and tactics used by foreign intelligence entities and industry competitors, and it provides guidance on how employees can protect themselves and the company.[208] As an industry leader in insider threat mitigation, Lockheed Martin recognizes the need to not only teach employees which behavioral indicators to look for but also to administer knowledge surveys to gauge changes in employee perceptions and overall program effectiveness.[209]

The final step (five) in its ITDP is to establish a governance structure. The purpose is to ensure the ITDP operates legally and compliant with company regulations. A crucial aspect is also to setup an oversight process and procedures for internal investigations.[210] Privacy considerations are important throughout the steps of the ITDP, especially in the last step. For example, how is the data collected from step two (leveraging technology) viewed and shared? Another potential issue involves privacy if employees are believed to pose an insider threat or demonstrates indicators of an insider threat on the company's network, yet further investigation into their actions reveals the

[206] Ibid., 4.

[207] Ibid.

[208] Ibid.

[209] Ibid.

[210] Ibid., 5.

employee is not an insider threat concern. These are all issues the company works out in advance across its various departments to ensure proper handling of employees' privacy. Lockheed Martin does not openly publish its privacy policies, but it clearly engages its legal team as a partner in the ITDP continually.

Another point of interest is the company's integration of CI and insider threat detection. First, the company performs internal investigations by utilizing a cadre of experienced CI professionals.[211] This same CI cadre takes the lead on insider threat education, mitigation, detection, *and* investigations. Based on the publicly available literature, it appears that Lockheed Martin obliterates the line between security and CI and integrates the two concepts. For the most part, at least organizationally speaking, the company seems to house these functions under its overall CI program.[212]

Without access to company resources, it is difficult to ascertain for certain how Lockheed Martin divides security functions between other departments and its CI staff, but we can derive reasonable conclusions based on the information on its public webpage. First, as discussed earlier in this section, Lockheed Martin's human resource department represents the first security measure for new employees since it processes each employee's government security clearance and requires an annual security clearance revalidation.[213] These types of government security clearance investigations can be considered a form of employee vetting and re-vetting. Second, the company employs information technology system monitoring. Its internal (intranet) login page can be accessed on the World Wide Web through a simple search. Upon opening the page, there is a disclaimer that employees should have no expectation of privacy on the company network and their usage "may be monitored and recorded by system personnel or by third

[211] Thomas and Rishikof, "Counterintelligence and Insider Threat," 5.

[212] Ibid., 5.

[213] "Security Clearance Connection," Lockheed Martin, accessed April 29, 2017, https://lockheedmartin.com/us/employees/security-clearance.html.

parties."[214] From this information, it appears Lockheed Martin spreads out security functions across different company departments and that a cadre of CI professionals design policy, educate the workforce, and perform follow up investigations when suspicious activity is detected.

2. Targeting the Unwitting Insider Threat

This thesis has discussed examples of insiders whose actions were specifically driven to further their own end goals whether they were working for a foreign intelligence entity, terrorist organization (or ideology), or were criminally motivated. However, an insider threat can also involve an unwitting insider. This occurs when an individual is "deceived into advancing our adversaries' objectives without knowingly doing so."[215] In today's digital world, unwitting insiders are often targeted through cyber social engineering schemes designed to get their login credentials to a company or agency's intranet and access to the sensitive data that resides on internal networks.

In 2016, a Chinese citizen with permanent residency in Canada pled guilty to charges surrounding a cyber-hacking scheme that resulted in the theft of trade secrets from American defense contractors, including Lockheed Martin.[216] Su Bin utilized at least one unwitting insider at Lockheed Martin to gain access to the company's digital files. According to a U.S. Attorney's Office press release from the Central District of California, Su Bin "worked with two unindicted co-conspirators based in China to infiltrate computer systems and obtain confidential information about military programs, including the C-17 transport aircraft, the F-22 fighter jet, and the F-35 fighter jet."[217] The

---

[214] "Lockheed Martin Internal Login," Lockheed Martin, 2017, https://lm-sts.p.external.lmco.com/adfs/ls/?wa=wsignin1.0&wtrealm=http%3a%2f%2fexo-sts.p.external.lmco.com%2fadfs%2fservices%2ftrust&wctx=d6510c08-8e1c-4a1d-bc36-103ca10229e3&wct=2017-10-06T00%3a35%3a33Z&whr=http%3a%2f%2flm-sts.p.external.lmco.com%2fadfs%2fservices%2ftrust.

[215] NCSC, *National Insider Threat*, 2.

[216] Justin Ling, "Man Who Sold F-35 Secrets to China Pleads Guilty," *Vice News*, March 24, 2016, https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty.

[217] "Los Angeles Grand Jury Indicts Chinese National in Computer Hacking Scheme Allegedly Involving Theft of Trade Secrets," press release, U.S. Attorney's Office, Central District of California, June 22, 2015, https://www.justice.gov/usao-cdca/pr/los-angeles-grand-jury-indicts-chinese-national-computer-hacking-scheme-allegedly.

F-22 and F-35 are both designed and manufactured by Lockheed Martin.[218] The charges against him relate to "unauthorized computer access, a conspiracy to illegally export defense articles and a conspiracy to steal trade secrets."[219]

Su Bin was the owner of a Chinese aviation company with offices located in Canada. He was also the central figure in an international hacking organization that stole sensitive digital data from American defense contractors. Su Bin worked with two officers from the Chinese military who facilitated the technical aspects of the operation.[220] Their strategy was remarkably simple and effective. Specific procedures and tactics have not been revealed by investigators to the public, but there is enough detail to ascertain the basics of the operation. First, the unwitting insider was specifically (by name) targeted by the perpetrators as someone reasonably believed to have access to sensitive data of value. Next, one of the military officers involved sent phishing emails to the targeted employee. The senders socially engineered the emails to have the appearance of a legitimate email from a colleague.[221] The email directed the employees to a website under the hackers' control, and this enabled them to gain access to Lockheed Martin's systems to start installing malware. Once in the system, the military officers copied files to send to Su Bin, who translated the files and helped direct further theft efforts.[222]

The effectiveness of this operation (before it was uncovered) is only eclipsed by its own brilliance and simplicity. Instead of exposing an intelligence agent to recruit an insider at Lockheed Martin, those involved instead duped a company employee into granting them digital access to the information they sought. This operation reflects the reality of today's digital world and the serious impact of an unwitting insider threat. In the Su Bin hacking scenario, there were no behavioral indicators to predict which employee had become the unwitting insider threat. Education, awareness, and a proactive

---

[218] Matt Apuzzo, "Chinese Businessman Is Charged in Plot to Steal U.S. Military Data," *The New York Times*, July 11, 2014, Online edition, https://www.nytimes.com/2014/07/12/business/chinese-businessman-is-charged-in-plot-to-steal-us-military-data.html, sec. Business D.

[219] "Los Angeles Grand Jury Indicts Chinese National."

[220] Ling, "Man Who Sold F-35 Secrets to China."

[221] Ibid.

[222] Ibid.

culture of threat recognition are perhaps the only way to prevent an employee from being coopted into an insider threat.

3. Conclusion—Organizational Culture and CI Are Key

Lockheed Martin's insider threat detection program is an interesting example to study because it combines its security programs with a robust CI program. This is noteworthy because Lockheed Martin is a private company and not a member of the IC, yet it operates a very CI-focused insider threat program. It has an excellent organizational structure and response policy that seems keenly aware of what can be handled "in house," and when the CI investigation meets the threshold for FBI involvement. However, the key component is the establishment of a security and insider threat awareness culture considered by many to be a model program for both industry and government.

The following chapter offers analysis of the different policies identified within each of the reviewed organizations. There are strengths, weaknesses, and limitations inherent in any approach to the insider threat problem. Are there additional options for TSA to consider to strengthen its programs, and even more importantly, is TSA even allowed to perform certain countermeasures? These issues are explored next.

IV. ANALYSIS AND FINDINGS: WHAT DOES THE IDEAL INSIDER THREAT PROGRAM LOOK LIKE?

The policies and practices of the organizations identified in the previous chapter suggest there are three primary areas of focus for preventing, detecting, mitigating, and investigating insider threats. These can be broken out into the following:

1. Security programs
2. Counterintelligence
3. Organizational culture

A reciprocally supportive construct across these three areas is key for a balanced approach to the insider threat problem.

A. SECURITY PROGRAMS

All the organizations reviewed in the previous chapter view security programs as a critical cornerstone to deterring and detecting insider threats. Security programs are defensive and akin to a goalie patrolling the net. They know what they are defending against and the area (goal) they are protecting. Unfortunately, even the best goalies from time to time have the ball kicked past them.

At their core, security programs can be split into two main categories: personnel vetting and access control. Personnel vetting ensures there is a review of an employee's suitability and trustworthiness for employment. When it comes to insider threat prevention, this is often the first step. Before an employees receive access to sensitive areas or systems, they must first pass a background check. For all the organizations reviewed in this thesis, the background check is designed to ensure trustworthiness and the absence of any concerning criminal or terrorism records relevant to the applicant. For the U.S. based organizations, the background check is often in the form of a government security clearance designed to ensure each employee "shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United

States."[223] According to a 2015 DHS OIG report entitled *TSA Can Improve Aviation Worker Vetting*, the inspector general determined TSA does an effective job of aviation worker vetting against terrorism watchlists on an initial and recurring basis.[224] This is especially impressive given the sheer number of employees and aviation workers they have to vet.

As a function of most U.S. government security clearances, a periodic reinvestigation usually occurs at an interval of every five to 10 years.[225] From the insider threat prevention standpoint, this period of re-vetting is designed to detect and deter an insider who may pose a threat and who already has been employed for several years. On the surface, this measure makes sense since the research demonstrates that 76 percent of insider who became threats decided to act after their they had already been employed.[226] In other words, their employment was not a purposeful penetration of the organization designed to gain access in accordance with a preexisting plot. It is at some point during their employment that three out of four insiders who become threats decide to carry out an illegal plot. One can conclude that a pending reinvestigation has a deterrent influence on some potential insider threats. TSA's re-vetting programs, whether for aviation workers or their own employees, are continuously improving, such as the increasing adapting of the FBI Rapback program.[227]

The standard for most IC agencies (including the FBI) is regular and recurring employee polygraph examinations. There is some debate, however, as to whether a polygraph has a CI function or security function. This section includes discussion on polygraph program here in the context of it being a security program since the FBI houses it polygraph program in its security division. Due to fallout from the Hanssen

---

223 "About Investigations," National Background Investigations Bureau, accessed November 11, 2017, https://nbib.opm.gov/about-us/about-investigations/.

224 Roth, *TSA Can Improve*, 4.

225 "Frequently Asked Questions: Investigations," Office of Personnel Management, accessed November 11, 2017, https://www.opm.gov/faqs/QA.aspx?fid=cb3cafac-1e73-4a6b-bd88-a3adad355390&pid=6bd77335-4541-4109-919b-cf43d01441c7&result=1.

226 CPNI, *CPNI Insider Data Collection*, 4.

227 Katko, *America's Airports*, 14.

case, the FBI now requires a polygraph as part of the standard five-year background reinvestigation for employees.[228] The implied assumption is that a regular polygraph has the capability to detect an insider threat, although there is little data available to substantiate this. Still, employee polygraphs can be considered a common practice to detect insider threats. TSA does not appear to conduct employee polygraphs, nor is there a strong argument for doing so now as TSA does not face the same foreign intelligence entity threat as the FBI and it already performs in-depth criminal records checks.

Access control, both physical and virtual on information technology systems, is the second critical component of insider threat security programs. All the organizations reviewed in Chapter III either have or encourage a form of information technology system monitoring as one of the backbone security programs in the twenty-first century. E.O. 13587 is very explicit about this and mandates all U.S. executive branch agencies apply such protections to prevent the inappropriate disclosure of classified and sensitive data taken from information technology systems.[229] TSA appears to comply with this section of E.O. 13587.

Physical access control is another critical component of an insider threat program. Physical access control ensures only adequately vetted personnel can physically enter (access) areas that correspond with their duties and job requirements. These controls add a layer of security and an opportunity to discover insiders posing threats attempting to get into places for which they have no workplace requirement. However, the very definition of an insider threat implies an ability to work around physical access controls because the insider has been granted legitimate, employee access to controlled areas.[230] It is difficult to evaluate TSA's performance in this area because it mostly regulates physical access controls only, and airport industry officials agree that there are no best practices to apply nationwide due to differences in layout, operation tempo, and feasible security measures.[231]

---

[228] Fine, *A Review of the FBI's Performance*, 22.

[229] Exec Order No. 13,587.

[230] NCSC, *National Insider Threat*, 1–2.

[231] Grover, *Aviation Security*, 41.

Overall, good security programs are essential to detecting and deterring an insider threat. These programs serve as a baseline for doing as much due diligence as possible so that employees gaining physical or virtual access to sensitive areas or systems are loyal and do not intend to become an insider threat. As discussed at the beginning of the chapter, security programs are a protective measure, a defensive tactic. Security programs beg the follow-up question: what are the next steps if a security program detects activity indicative of an insider threat?

B. COUNTERINTELLIGENCE

If security programs are the shield, then CI programs are the sword. These operations are most efficient once an employee exhibits insider threat indicators. Lockheed Martin considers this step a "soft inquiry" designed to peel back the anomalous behavior to see if there is a nefarious intent.[232] CI operations are used by I&A, the FBI, and Lockheed Martin to address the insider threat problem once a security program develops a lead. This is also the perspective of the ODNI. Published by ODNI, the 2016 *National CI Strategy* discusses the natural partnership and handoff between security and CI programs. It states, the "U.S. government must strengthen its CI programs and processes to adapt to the complexity of foreign intelligence entity and insider threats."[233] The CI strategy document also acknowledges the essential role of integrating security programs and CI as a force multiplier, stating, "This strategy acknowledges the critical role of security programs in contributing to the integrity of our CI efforts."[234]

CI is inherently going to involve a level of invasive intelligence collection. U.S.C. Title 50, § 3001 defines it as:

> …information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers,

---

[232] Kopp, "How Lockheed Martin."

[233] Office of the Director of National Intelligence [ODNI], *National Counterintelligence Strategy of the United States of America 2016* (Washington, DC: Office of the Director of National Intelligence, 2016), 8.

[234] Ibid., 2.

> organizations or persons, or their agents, or international terrorist groups or activities.[235]

Insiders associated with criminal organizations do not fit neatly into this definition of CI, but the CI tactics are the same regardless of whether the insider is a terrorist or a criminal.

U.S.C Title 50 authorizes a CI function for IC members only. For example, performing an intelligence mission, FBI units are explicitly given authorization to "(c)ollect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions."[236] According to the Office of the Law Revision Counsel of the U.S. House of Representatives, "The United States Code is a consolidation and codification by subject matter of the general and permanent laws of the United States."[237] Therefore, Title 50 contains at least some of the legal authority for IC agencies to conduct CI activities directed at mitigating insider threats. Determining exactly how much authority Title 50 provides for CI exceeds the scope of this thesis, but it does appear that Title 50 grants specific authorization for CI activities to certain federal agencies.

This delineation is necessary to point out because TSA is not included as a member of the IC and therefore does not have Title 50 authority to conduct CI activities. Further analysis of whether other legal authorities exist that could grant CI power to TSA is a research gap that could be the subject of future research. For now, given TSA does not have specific statutory authorization to conduct a CI program and is not designated as an IC member, it is safe to assume TSA is not able to use CI investigations or a CI collection program to investigate and develop intelligence collection operations against insider threats.

As a counterpoint, Lockheed Martin relies very heavily on its internal CI program for insider threat investigation even though it is not a member of the IC. It is difficult to make an apple-to-apple comparison between TSA, a government agency, and Lockheed

---

[235] War and National Defense, U.S.C. Title 50 § 3001 (2011), 437.

[236] Ibid., 435.

[237] "U.S. House of Representatives," Office of the Law Revision Council, U.S.C. April 9, 2017, http://uscode.house.gov.

Martin, a private company; however, Lockheed Martin's utilization of CI as an internal tactic without conducting intelligence collection operations is worthy of emulation in TSA since it would serve as a method for TSA to incorporate CI principles and "soft inquiries," without overstepping its authority by performing a domestic intelligence (CI) collection operation. As a key privacy consideration, Lockheed Martin's CI program does not collect any information not already gathered through other corporate initiatives.[238] In contrast, TSA would need to refer a more complicated CI operation involving domestic intelligence collection against foreign intelligence entities to the FBI.[239] This appears consistent with TSA's policy of referrals of insider threat cases (such as the Terry Lee Loewen case discussed earlier) to the FBI for further investigation.

Historically, the FBI has addressed insider threats as a CI issue. Since it is a law enforcement agency and a member of the IC, it has more options for pursuing insider threat investigations than TSA does. One of these options is the use of intrusive CI collection methods, such as the previously discussed controlled source and double agent operations.[240] CI methods are one tactic that could conceivably assist TSA with workers in the aviation environment. The ability to run a controlled source operation in the aviation domain could lead to developing more leads and cases to uncover possible insider threats. This method could have been of use at Minneapolis-St. Paul International Airport a few years ago, for example, and it may have helped to identify radicalized individuals before they were ready to fight with terrorist organizations overseas.

As an IC member, I&A also appears to be developing a CI capability for the entire DHS apparatus. It is not yet clear how aggressive I&A will be in using its CI staff for insider threat intelligence collection and investigations, but it is worthwhile to consider if TSA can tap into I&A CI resources to conduct CI operations when a TSA security program or lead hints at an insider threat within the aviation system. According to 2016 testimony to the House Subcommittee on Counterterrorism and Intelligence testimony, then Chief Intelligence Officer for DHS Francis Taylor stated that one of the

---

[238] Thomas, "Lockheed Martin Counterintelligence," 12.

[239] War and National Defense, U.S.C. Title 50 § 3001 (2011), 435.

[240] Reagan *Terms and Definitions,* 52.

goals of the I&A CI program is to "deepen our understanding of threats posed by foreign intelligence entities and insider threats to DHS."[241] An additional goal is proactive training development and "effective investigative efforts."[242] It is reasonable to conclude the I&A CI program would allow for CI investigations across the different DHS components shortly.

C. ORGANIZATIONAL CULTURE

Both CPNI and Lockheed Martin champion the principle of insider threat detection and mitigation through corporate culture. This concept is surprisingly easy to quantify. Only six percent of insider threat cases from a CPNI study indicate the insider joined its organizations with the intent to become an insider to pose a threat, meaning deliberate infiltration.[243]In contrast, three out of four insiders who posed threats gained employment with CPNI first and then noticed opportunities to exploit their employee access to sensitive areas and systems.[244] This statistic speaks for itself as to the importance of establishing an organizational culture that not only "hardens the target" as deterrence, but one that also minimizes the motivations of employees as insiders to become threats during employment. The same CPNI study found the primary reason for becoming an insider posing a threat is financial gain; 47 percent of insiders cited this as their primary incentive. Ideology came in second at 20 percent,[245] which is more difficult to counter through cultural change since we can assume their ideology clashed with the organization's values or they would not have chosen to become an insider posing a threat. The final leading factor is a "desire for recognition" at 14 percent,[246] and this can be addressed through management practices.

These statistics help drive home the importance of increasing workplace satisfaction and morale as insider threat prevention measures. Often, these are human

---

[241] Taylor, Hayes, and McComb, *Counterintelligence and Insider Threats*, 3.

[242] Ibid.

[243] CPNI, *CPNI Insider Data Collection*, 4.

[244] Ibid.

[245] Ibid.

[246] Ibid.

resources and management issues, not security or CI related problems. When the organizational culture fails the employees in these areas, the result can be an employee actively wishing to harm the organization. More study is required to understand the financial motive of the 47 percent that cited an economic driver as their goal for becoming an insider threat.[247] It is not clear if a slightly higher salary or better workplace morale could have dissuaded these from their threatening activities.

Regardless, establishing a workplace culture of insider threat awareness represents a best practice because it helps make the organization a "hardened target." In particular, Lockheed Martin has done an excellent job of marrying a threat awareness culture with CI investigations. The company's security programs encourage "engaged employees" to report on suspicious indicators and develop potential leads. These cultural changes took about two years to accomplish and resulted in the termination of 13 employees who had been displaying insider threat indicators and appeared ready to commit nefarious acts.[248] Lockheed Martin changed its threat awareness culture by educating employees on insider threat signs while tying the threat to national security, revenue, and job implications for its employees.[249]

None of the literature on TSA's programs mention organizational culture as an insider threat deterrent. This gap is one area where TSA can further enhance its strategy to counter insider threats within its agency.

D. CONCLUSION—FINDING THE RIGHT BALANCE

The insider threat mitigation measures analyzed in this chapter represent the three primary schools of thought on how to counter insider threats. One of the weaknesses of the TSA, I&A, and even the FBI insider threat program is the focus on detection and response. This focus assumes there will be an ideologically or criminally driven individual lurking in the shadows and waiting for an opportunity to leverage legitimate employee access to further a plot. While this may be true to an extent, it tends to ignore

[247] Ibid.

[248] Thomas, "Lockheed Martin Counterintelligence."

[249] Ibid.

the effect of an organization's cultural factors in preventing insiders posing threats from acting because they have a security awareness ethos with full support across the entire leadership apparatus. Thorough cultural engagement is where it becomes clear that Lockheed Martin's ITDP represents the most comprehensive insider threat program among the organizations this thesis reviews. Finding the right balance between deterrence and response is good policy for the insider threat problem.

The next chapter discusses some specific recommendations for TSA to enact to improve upon its insider threat program while also identifying areas for further research that could identify more measures for TSA to adopt. The research does not reveal a perfect formula for mitigating insider threats within an organization. However, it is evident that a balanced approach starting from prevention to detection to response is needed.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. RECOMMENDATIONS AND DISCUSSION

There is no "one size fits all" approach to creating an insider threat program. Insider threat is ultimately a "people" problem and not a distinct information technology problem, access problem, or CI problem. The vulnerabilities that an insider threat program attempts to reveal are the same vulnerabilities that an insider posing a threat is ideally positioned to exploit. This ultimately becomes an issue of identifying employee intent and attempting to peek into the future. Still, there are a variety of measures that can be taken to improve TSA's insider threat program.

Stated simply, the first goal of an insider threat program should be prevention by not employing an insider threat in the first place. The next goal is to deter the insider threat from acting owed to a perceived likelihood of discovery. Finally, if an insider cannot be deterred, then they need to be detected and investigated. A comprehensive insider threat program must incorporate all three of these goals.

TSA is inherently limited in its ability to perform offensive measures due to its lack of law enforcement and intelligence collection authorities. With a little creativity, however, there are still many measures TSA can enact to remain proactive in addressing the insider threat.

1. Recommendation 1: Increase the Use of the TSA VIPR Program in the Airport Environment

There was a broad consensus from the Aviation Security Advisory Committee in 2015 that the expectation for physical screening of aviation workers on any given workday is an excellent insider threat prevention tool.[250] Although more study regarding the expectation of possible screening vice the certainty of physical screening each day needs to be conducted in order to determine if this assumption is correct, it is within the realm of good sense to assume that increases in random and unpredictable physical

[250] Aviation Security Advisory Committee, *Final Report*, 3.

screening of aviation workers can increase the expectation they will be screened on any given day, thereby providing a deterrent effect.

To accomplish this, TSA should increase its use of the VIPR program to deploy a more diverse set of assets to operate random physical screening checkpoints. For example, TSA explosives detection canine teams can be randomly placed at various access points at differing times to screen aviation workers and their work bags. Federal air marshals can increase random ID checks and provide a visible presence to escalate the perception that law enforcement is monitoring all areas within the SIDA zones. VIPR teams give TSA more resource options for random aviation worker screening and can help mitigate the resource drain on the transportation security officer workforce from having to perform this function. As a security program, VIPR provides the benefit of additional physical screening and access control measures to detect and mitigate insider threats. Equally important is a random law enforcement presence in the SIDA zones to deter aviation workers from heading down the path to becoming insider who pose threats.

Since TSA already operates the VIPR program, there are no immediately visible barriers to implementation from TSA's perspective. Using VIPR operations to increase the expectation among aviation workers of physical and unpredictable screening is supported by the airport operators and airlines.[251] This measure would likely receive widespread industry support based on feedback from the 2015 Aviation Security Advisory Committee report. The working group requested that TSA coordinate any access control and aviation worker physical screening procedure changes with the local airport stakeholders so they have an opportunity to provide feedback.[252] Its recommendation for a "community-driven" approach is a good long-term practice for TSA when increasing VIPR operations. Good coordination with local airport operators and stakeholders should help TSA avoid unintended consequences and industry resistance.

[251] Ibid.

[252] Ibid.

2. Recommendation 2: Adopt CPNI's Motivation Project to Identify If There Are Tangible Areas for Cultural Change

TSA should consider committing to a long-term initiative to measure the levels of motivation and morale within its workforce. Conceivably, this will help TSA develop and fine tune the change requirements needed within the organization to become a high performing security culture capable of mitigating the insider threat through awareness and employee engagement on the issue. On the other hand, such an initiative might also indicate that TSA has already achieved a strong security culture requiring few changes. Either way, it is difficult to measure without undertaking this initiative. CPNI already has a good model to emulate for this initiative in its Motivation Project, and it could be a good starting point for TSA to undertake a similar measure.

TSA should also adapt CPNI's "Motivation Project" for its external stakeholders. Similar to CPNI's outreach to other United Kingdom critical infrastructure facilities, TSA could also become the "consultant" on this issue to inspire cultural change not just within TSA but within the entire public-private aviation domain. TSA could offer and implement a survey and follow up analysis to help drive the organizational cultural changes needed to lead to better security awareness among aviation workers.

Implementation of a large-scale workforce survey will require broad management buy in within TSA as well as proactive communication to ensure the agency is aware of the long-term goals of this project. It is unclear what the costs associated with a long-term workforce survey of this magnitude are. Fiscal restraints have the potential to become a significant implementation issue if there is not leadership buy in across TSA for this initiative. Hopefully, this hurdle will naturally be resolved by enacting recommendation 3, described below.

3. Recommendation 3: Utilize Lockheed Martin's "Five Steps to Success" as a Baseline for Internal Review

The literature reviewed in this thesis demonstrates that including a policy of continuous internal evaluation of anomalous employee behaviors is healthy for an insider

threat program.[253] Employees are ideally positioned to identify new areas of vulnerability and concerning coworker behaviors. They should be able to proactively discuss these issues with management to preemptively address the problem as new vulnerabilities are discovered. For example, the technology to monitor employee behavior within an organization's information technology systems is a twenty-first century practice that has become more common as more sensitive and classified information has gone digital. TSA should work toward a holistic approach to the insider threat problem that engages the entire workforce and management to incorporate "buy in" among the various functions within TSA.

The cornerstones of Lockheed Martin's Insider Threat Detection Program (ITDP) represent the most comprehensive recommended outline for TSA's insider threat program. As described by Lockheed Martin, the ITDP is built around the following five key areas:

1. Gain leadership support
2. Leverage the latest technology
3. Develop a communications plan
4. Execute a training and awareness campaign
5. Establish a governance structure.[254]

The intent behind this recommendation is to further institutionalize the insider threat program in TSA.

Barriers for implementation of an insider threat program at TSA should be minimal. This does not require additional intelligence or law enforcement authorities and avoids political interagency problems since the changes will take place within TSA only. Internally, implementation requires leadership buy in, proactive communication vertically and horizontally across TSA personnel, and employee surveys to help identify baseline knowledge, as noted in the previous recommendation. Costs are also minimal since the

[253] ODNI, *National Counterintelligence Strategy*, 4.

[254] Lockheed Martin, *5 Steps to Develop*, 3.

five key areas center mostly on establishing agency-wide support and awareness of the insider threat.

4. Recommendation 4: Create or Hire a Cadre of CI Staff at TSA Headquarters to Develop Insider Threat Programs and Perform "Soft Inquiries"

One of the key advantages of the Lockheed Martin ITDP is full integration of its CI cadre within each stage of its insider threat policy development. As a private company, Lockheed Martin can work unilaterally in this regard except that it must refer insider threat cases to the FBI for prosecution since it is not a law enforcement or a Title 50 agency. However, its CI professionals can conduct the initial investigation and also develop the front-end policy, training, and procedures for the company's insider threat programs in the context of program security and CI. Within this example, there is some applicability to TSA. The agency could similarly hire CI professionals to develop TSA's internal policies and programs, including internal investigation referrals. Like Lockheed Martin, TSA would at some point need to hand over an investigation to the FBI for further action and prosecution, but it could develop the investigatory leads ("soft inquires") and determine the veracity of the cases internally first.

Implementation should not be too challenging. DHS I&A is already in the process of embedding experienced CI officers within each DHS operational component.[255] The primary purpose is to help counter foreign intelligence entity threats within the DHS components. However, this resource is by nature dual purpose since foreign intelligence entities often recruit an insider threat within a targeted organization (often referred to as the "CI insider threat").[256] TSA should leverage this resource to assist in hiring (or training) additional CI officers. By performing only initial soft inquiries, TSA avoids over extending itself into the FBI's lead CI role in the United States. As a bonus, this process could ensure more soft inquiries are performed and only the cases meeting the threshold of a foreign intelligence entity issue or an insider threat prosecution are referred to the FBI, thus helping to preserve FBI resources. It is conceivable there could be some

[255] Taylor, Hayes, and McComb, *Counterintelligence and Insider Threats*, 4.

[256] Vickers, *Department of Defense Instruction*, 13.

pushback from the FBI based on a misperception of the intent behind the soft inquiry. It is not proposed to extend into the FBI's lead CI role in the United States. Proactive soft inquiries could lead to more referred cases to the FBI. With some proactive communication by I&A and TSA with the FBI, pushback could be minimized.

B. AREAS FOR FURTHER RESEARCH

This thesis largely serves as a starting point for TSA to begin building on its insider threat security programs. There might be a few areas where TSA can become a little more aggressive and independent in developing a CI program, but further research is required to determine the legality of such operations. The focus of the proposed research below is geared towards exploring what can be done to provide more authority to TSA and thus reduce TSA's reliance on other agencies for CI operations to counter insider threats.

1. Are there other legal authorities such as the ATSA or E.O. 12333 that TSA can leverage for justification to conduct its own CI operations leading to domestic intelligence collection or to a prosecution?
2. Is there legal authority that TSA's Federal Air Marshal Service can use to execute CI operations in the same way described above?
3. Can TSA work with I&A's CI officers to conduct similar CI operations under Title 50 authority on its employees and contractors?[257]

C. CONCLUSION

Successful insider threat programs require a strong balance between security, CI, and organizational culture. The recommendations presented in this chapter are designed to be immediately implementable and will help TSA fine tune its defensive programs while initiating the beginning of an offensive campaign in the form of a CI program. The end goal should be to drive security and CI programs to a point at which they intersect and seamlessly feed each other. This is where the NCSC believes the solutions are to counter an organization's adversaries, including insider threats.[258]

[257] War and National Defense, U.S.C. Title 50 § 3001 (2011), 435.

[258] "How We Work," NCSC.

The importance of TSA taking immediate actions to develop robust insider threat programs cannot be overstated as there are more than 450 federalized airports tucked into every part of the United States. These airports connect people, goods, and services and are a key component of our nation's critical infrastructure.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Apuzzo, Matt. "Chinese Businessman Is Charged in Plot to Steal U.S. Military Data." *The New York Times*, July 11, 2014. https://www.nytimes.com/2014/07/12/business/chinese-businessman-is-charged-in-plot-to-steal-us-military-data.html.

Ashford, Warrick. "Is UK Critical National Infrastructure Properly Protected?" *Computer Weekly*, March 3, 2011. http://www.computerweekly.com/news/1280097313/Is-UK-critical-national-infrastructure-properly-protected.

Associated Press. "ISIS Leader Encourages Lone Wolf Attacks on Civilians in Europe and U.S." *The Guardian*, May 22, 2016. https://www.theguardian.com/world/2016/may/22/isis-leader-civilian-lone-wolf-attacks-us-europe.

Aviation Security Advisory Committee. *Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control*. Arlington, VA: Aviation Security Advisory Committee, 2015.

Baskas, Harriet. "How Many People Does It Take to Run an Airport?" *USA Today*, March 30, 2016. https://www.usatoday.com/story/travel/flights/2016/03/30/airport-workers-employees/82385558/.

Bay City News. "TSA Screeners Accused of Drug Smuggling Conspiracy." March 6, 2015. http://abc7news.com/news/tsa-screeners-accused-of-drug-smuggling-conspiracy/548594/.

BBC News. "Terror Plot BA Man Rajib Karim Gets 30 Years." March 18, 2011. http://www.bbc.com/news/uk-12788224.

Bergen, Peter. "How Big of a Threat Is Al-Shabaab to the United States?" *CNN*, February 22, 2015. http://www.cnn.com/2015/02/22/opinion/bergen-al-shabaab-threat/index.html.

Black, Alan. "Managing the Aviation Insider Threat." Master's thesis, Naval Postgraduate School, 2010.

Bull, Kylie, and Ben Vogel. "Daallo Airlines Bombing Investigation Focuses on Insider Threat." *IHS Jane's 360*, February 9, 2016. http://www.janes.com/article/57845/daallo-airlines-bombing-investigation-focuses-on-insider-threat.

Centre for the Protection of National Infrastructure. *CPNI Insider Data Collection Study: Report of Main Findings*. London: Centre for the Protection of National Infrastructure, 2013.

———. *Investigating Employees of Concern: A Good Practice Guide*. London: Center for the Protection of National Infrastructure, 2011.

———. *Motivation within the Security Industry*. London: Centre for the Protection of National Infrastructure. https://www.cpni.gov.uk/.../documents/52/73/guard-force-motivation.pdf.

———. *Personnel Security: An Ongoing Responsibility-Understanding Insider Threats-and Minimizing the Risk*. London: Center for the Protection of National Infrastructure, 2015. https://www.cpni.gov.uk/system/files/documents /5b/04/ongoing-personnel-security-infographic.pdf.

Chesney, Robert. *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*. Public Law and Legal Theory Research Paper Series. Austin, TX: University of Texas School of Law, 2012.

CNN. "Ex-FBI Spy Hanssen Sentenced to Life, Apologizes." May 14, 2002. http://www.cnn.com/2002/LAW/05/10/hanssen.sentenced/index.html?_s=PM:LAW.

Deffer, Frank. *Transportation Security Administration Has Taken Steps to Address the Insider Threat but Challenges Remain*. Washington, DC: U.S. Department of Homeland Security, Office of the Inspector General, 2012.

Edwards, Charles K. *Efficiency and Effectiveness of TSA's Visible Intermodel Prevention and Response Program Within Rail and Mass Transit Systems*. Washington, DC: U.S. Department of Homeland Security, Office of the Inspector General, 2012.

Federal Bureau of Investigation. *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy* [brochure]. Washington, DC: Federal Bureau of Investigation, 2011. https://www.fbi.gov/filerepository/insider_threat_ brochure.pdf/view.

Fine, Glenn A. *A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen*. Washington, DC: U.S. Department of Justice, 2003.

Grover, Jennifer A. *Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates*. Washington, DC: U.S. Government Accountability Office, 2016.

Katko, John. *America's Airports: The Threat from Within*. Washington, DC: House Homeland Security Committee, 2017.

Kopp, Emily. "How Lockheed Martin Sold Employees on an Insider Threat Program." *Federal News Radio*, October 30, 2015. https://federalnewsradio.com/defense-industry/2015/10/lockheed-martin-sold-employees-insider-threat-program/. program/.

Ling, Justin. “Man Who Sold F-35 Secrets to China Pleads Guilty.” *Vice News*, March 24, 2016. https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty.

Lockheed Martin. *5 Steps to Develop a Successful Insider Threat Detection Program*. Bethesda, MD: Lockheed Martin, 2015. http://informationsecurity.report/Resources/Whitepapers/2e8a0821-6982-4666-8e46-bd7153a6989f_5%20Steps%20to%20Develop%20a%20Successful%20Insider%20Threat%20Detection%20Program.pdf,

———. *Counterintelligence Awareness: Capability Without Compromise*. Bethesda, MD: Lockheed Martin, 2015. https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/clearanceconnection/CI_Awareness_briefing.pdf.

Lucaccioni, Cassandra. “61st Terrorist Plot Against the U.S.: Terry Lee Loewen Plot to Attack Wichita Airport.” *The Issue Brief*, no. 4110 (December 2013). http://www.heritage.org/research/reports/2013/12/terry-lee-loewen-terrorist-plot-in-wichita-kansas-airport.

Mathews, Owen. “Metrojet Crash: Why The Insider Threat to Airport Security Isn’t Just Egypt’s Problem.” *Newsweek*, May 24, 2016. http://www.newsweek.com/2016/06/03/egyptair-metrojet-flight-9268-airport-security-462784.html.

MacFarlane, Scott. “Feds Investigating Whether Employee Was Plotting Attack on Homeland Security Officials.” *News4 I-Team*, June 21, 2016. http://www.nbcwashington.com/investigations/Feds-Investigating-Whether-Employee-Was-Plotting-Attack-on-Homeland-Security-Officals-383852591.html.

National Counterintelligence and Security Center. *National Insider Threat Task Force Mission Fact Sheet*. Washington, DC: National Counterintelligence and Security Center, https://www.dni.gov/files/NCSC/documents/products/National_Insider_Threat_Task_Force_Fact_Sheet.pdf.

Office of the Director of National Intelligence. *Countering Foreign Intelligence Threats: Implementation and Best Practices Guide*. Washington, DC: Office of the Director of National Intelligence, 2017. https://www.dni.gov/files/NCSC/documents/campaign/Guid_CFIT-Implementation-and-Best-Practices-Guide_2017-06-08_UNCLASS_LINKED.pdf.

———. *National Counterintelligence Strategy of the United States of America 2016*. Washington, DC: Office of the Director of National Intelligence, 2016.

Puleo, Anthony J. “Mitigating Insider Threat Using Human Behavior Influence Models.” Master’s thesis, Air Force Institute of Technology, 2006.

Randol, Mark A. *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress* (CRS Report No. 7–5700). Washington, DC: Congressional Research Service, 2010.

Reagan, Mark L. *Introduction to U.S. Counterintelligence-CI 101, a Primer*. Washington, DC: U.S. Department of Defense, 2005.

———, ed., *Terms and Definitions of Interest for Counterintelligence Professionals*. Washington, DC: Department of Defense, 2014.

Roth, John. *TSA Can Improve Aviation Worker Vetting* (OIG-15-98). Washington, DC: U.S. Department of Homeland Security, Office of Inspector General, 2015.

Sharkey, Joe. "Gun Smuggling on Plane Reveals Security Oversight." *The New York Times*, December 29, 2014. http://www.nytimes.com/2014/12/30/business/gun-smuggling-on-plane-reveals-security-oversight.html?_r=0.

Skinner, Richard L. *DHS Counterintelligence Activities*. Washington, DC: U.S. Department of Homeland Security, Office of the Inspector General, 2010.

———. *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening* (OIG-09-05). Washington, DC: U.S. Department of Homeland Security Office of Inspector General, 2008.

Tarry Jr., William E. *DHS Intelligence Enterprise*. Washington, DC: U.S. Department of Homeland Security, 2013.

Taylor, Francis, Robert Hayes, and Rich McComb. *Counterintelligence and Insider Threats: How Prepared Is the Department of Homeland Security?* Washington, DC: U.S. Department of Homeland Security, 2016.

Thomas, Douglas D. "Lockheed Martin Counterintelligence and Insider Threat Programs" Presented at Annual Industry Security Conference, Washington, DC, 2015. http://www.connectidexpo.com/creo_files/2015_day1/16.15%20Douglas%20D.%20Thomas%2023%20Mar%202015%20Connect%20ID%20Expo.pdf.

Thomas, Douglas D., and Harvey Rishikof. "Counterintelligence and Insider Threat Detection." Presentation for Government Contractors Forum, Security Clearance and Insider Threat Boot Camp, February 2016. http://m.acc.com/chapters/ncr/upload/Session-2-Insider_Threat_Program_Panel2_020916.pdf.

U.S. Department of Homeland Security, *Information Sharing and Safeguarding* (DHS Directive 262–05). Rev 00. Washington, DC: U.S. Department of Homeland Security, 2014.

———. *Insider Threat Program* (DHS Instruction 262–05-01). Washington, DC: U.S. Department of Homeland Security, 2015.

———. *Privacy Impact Assessment for the DHS Insider Threat Program*. Washington, DC: U.S. Department of Homeland Security, 2015.

U.S. Government Accountability Office. *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Perimeters and Access Controls*. Washington, DC: U.S. Government Printing Office, 2009.

Vickers, Michael J. *Department of Defense Instruction: Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat.* Washington, DC: U.S. Department of Defense, 2012. https://www.hsdl.org/?view&did=745624.

White House. *National Insider Threat Policy*. Washington, DC: White House, 2012.

Zamost, Scott, and Drew Griffin. "Despite Security Gaps, No Full Screening for Airport Workers." *CNN*, April 21, 2015. http://www.cnn.com/2015/04/20/travel/airport-workers-security-screening/index.html.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California