NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INSIDER THREAT: A CONSTANT PROBLEM WITH A CONTINUOUS APPROACH

by

Taj Mathew

March 2023

Co-Advisors: Robert L. Simeral (contractor)
Erik J. Dahl

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE INSIDER THREAT: A CONSTANT PROBLEM WITH A CONTINUOUS APPROACH	**5. FUNDING NUMBERS**
6. AUTHOR(S) Taj Mathew	
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.

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

13. ABSTRACT (maximum 200 words)

In 2001, the Transportation Security Administration (TSA) was created to secure all modes of transportation from external threats such as terrorists and other actors with malicious intent. Currently, the most dangerous threat to aviation security is an insider threat. What TSA can do better to address insider threats is the primary focus of this thesis. This thesis utilizes a comparative analysis to examine the insider threat programs at the Department of Defense and the Federal Bureau of Investigation in the United States and the Centre for the Protection of National Infrastructure in the United Kingdom to explore insider threat mitigation options for TSA. This thesis finds that TSA should establish a more thorough vetting of applicants and an ongoing review of current aviation employees. Accomplishing this recommendation will require multiple strategies, including establishing and strengthening partnerships to leverage expertise and maximize resources.

14. SUBJECT TERMS Transportation Security Administration, TSA, insider threat, polygraph, continuous evaluation, CE, intelligence community, security vulnerabilities, polygraph, background investigations, social media screening	**15. NUMBER OF PAGES** 107
	16. PRICE CODE

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

INSIDER THREAT: A CONSTANT PROBLEM WITH A CONTINUOUS APPROACH

Taj Mathew
Special Agent, TSA Investigations, Department of Homeland Security
BS, York College of Pennsylvania, 2005

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
March 2023**

Approved by: Robert L. Simeral
Co-Advisor

Erik J. Dahl
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In 2001, the Transportation Security Administration (TSA) was created to secure all modes of transportation from external threats such as terrorists and other actors with malicious intent. Currently, the most dangerous threat to aviation security is an insider threat. What TSA can do better to address insider threats is the primary focus of this thesis. This thesis utilizes a comparative analysis to examine the insider threat programs at the Department of Defense and the Federal Bureau of Investigation in the United States and the Centre for the Protection of National Infrastructure in the United Kingdom to explore insider threat mitigation options for TSA. This thesis finds that TSA should establish a more thorough vetting of applicants and an ongoing review of current aviation employees. Accomplishing this recommendation will require multiple strategies, including establishing and strengthening partnerships to leverage expertise and maximize resources.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACS	Automated Case Support
ATLAS	Advanced Threat Local Allocation Strategy
CE	continuous evaluation
CIA	Central Intelligence Agency
CPNI	Centre for the Protection of National Infrastructure
DCSA	Defense Counterintelligence and Security Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DISC	Detect, Identify, Secure, and Counter (Program)
DITMAC	DOD Insider Threat Management and Analysis Center
DOD	Department of Defense
e-QIP	Electronic Questionnaires for Investigations Processing
FAM	federal air marshal
FAMS	Federal Air Marshal Service
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
IC	Intelligence Community
IT	information technology
ITDS	insider threat detection system
ITP	Insider Threat Program
InTAP	Insider Threat Analysis Platform
ITRB	Insider Threat Risk Board
NIPA	National Policing Improvement Agency
NORTHCOM	Northern Command
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
ODT	ocular-motor deception test

OPM	Office of Personnel Management
PERSEREC	(Defense) Personnel and Security Research Center
PIN	personal identification number
SIDA	secure identification display area
TSB	Technical Services Branch
TSA	Transportation Security Administration
TSA INV	Transportation Security Administration Investigations
TWIC	Transportation Worker Identification Credential
UK	United Kingdom
ZTA	Zero Trust Architecture

EXECUTIVE SUMMARY

In 2001, the Transportation Security Administration (TSA) was created to secure all modes of transportation from external threats such as terrorists and other actors with malicious intent. Currently, the most dangerous threat to aviation security is an insider threat. Numerous recent incidents show that the people charged with protecting transportation security for the nation have exploited the access granted through their positions. In 2013, TSA created an Insider Threat Program (ITP), which involved processes to curb insider threats, but ITP has failed to fully detect and prevent them. Although TSA requires limited background checks and conducts randomized employee screenings, it lacks a strategic plan to guide its ITP and fully protect the agency.[1]

TSA can benefit from adopting the previously vetted and utilized policies and procedures of other security-based organizations. This thesis utilizes a comparative analysis approach to examine the insider threat programs at the Department of Defense (DOD) and the Federal Bureau of Investigation (FBI) in the United States and the Centre for the Protection of National Infrastructure (CPNI) in the United Kingdom (UK). The two U.S. agencies are appropriate for study because they each screen broad types of personnel and have previous experiences with damaging insider threats. The UK is an American ally with similar laws and threats. Employing the Star model for analysis, this thesis examines the screening strategies, policies, procedures, and technologies used by these organizations and explores the barriers and benefits to their adoption.[2] The methods of insider threat mitigation and detection vary significantly in implementation and effectiveness; however, the consensus is that insider threats are a tangible danger that needs to be addressed. In short, these organizations use continuous evaluation screening programs to mitigate insider threats.

[1] Triana McNeil, *Aviation Security: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals*, GAO-20-275 (Washington, DC: Government Accountability Office, 2020), https://www.gao.gov/products/GAO-20-275.

[2] Jay Galbraith, "The Star Model," Galbraith Management Consultants, accessed May 11, 2021, https://www.jaygalbraith.com/images/pdfs/StarModel.pdf.

While there is no "silver bullet" for combating insider threats and each organization has a diverse employee population, TSA can take additional steps to further protect the agency and the traveling public. The following are several recommendations that TSA can explore for implementation:

- Oversee a standardized pre-employment screening of 100 percent of transportation workers before onboarding.
- Enact random and periodic screenings of all TSA employees.
- Utilize partnerships to advance insider threat detection.
- Hire designated criminal investigators tasked specifically with investigating insider threats within TSA.

TSA is critical to keeping the traveling public safe through various tactics, including passenger and cargo screening, and other aviation security channels. Domestic extremism and violence, rather than foreign terrorism, are quickly morphing into TSA's greatest threat. The best way to protect TSA and the flying public is by thoroughly and continuously vetting all applicants and current aviation employees by mimicking the DOD's and FBI's personnel security procedures and looking to best practices implemented internationally, like those of CPNI. TSA will face hurdles in undertaking these policy changes, but the current TSA policy lacks the procedures and requirements to be effective.

ACKNOWLEDGMENTS

Completing coursework and this thesis would not have been possible without my lovely, amazing, and 100 percent supportive wife, Pamela. Over the past two years, you have always been by my side, encouraging me, supporting me, and believing in me. Over the past two years, I have been a complete stress ball, and you have put up with me. We have missed vacations, date nights, and quality time with family because of school. I don't know how I will return the grace and patience you have shown me.

I would like to thank my advisors, Dr. Erik Dahl and Robert Simeral, for taking me on in a rather unorthodox situation and being extremely understanding and helpful. Also, to Scott Martis, thank you for always working hard to take care of our class.

Last, I would like to thank my boss, Special Agent in Charge Mark Kreuziger, who supported me in attending school at the expense of being short-staffed. You supported me as an employee, student, and person.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Recent incidents show that some of the people charged with protecting transportation security for the nation have exploited the access granted through their positions. For example, in 2006, two federal air marshals (FAMs) were arrested for smuggling drugs, a large quantity of cash, and fraudulent identity documents into the United States.[1] More recently, in December 2020, 20 FAMs and their supervisors were disciplined for smuggling Viagra into the United States for personal use, which they had purchased from overseas locations at a significant discount and without a medical doctor's prescription.[2] The duties of TSA's FAMs include preventing and defeating hostile acts against aviation by monitoring passengers on domestic and international flights and, when necessary, taking enforcement actions. FAMs have taken advantage of their ability to bypass international and domestic security when traveling to smuggle drugs and other illicit materials into the country.

During a routine employee misconduct investigation in 2016, TSA Investigations discovered a major insider threat in Puerto Rico involving a drug trafficking organization. According to the Department of Justice, "During the course of the conspiracy, the defendants smuggled suitcases, each containing at least 15 kilograms of cocaine, through the TSA security system at the Luis Muñoz Marín International Airport."[3] The perpetrators had successfully engaged in smuggling from 1998 to 2016. Until TSA investigators identified specific insider threats, every TSA employee at the airport had been a potential

[1] Villarreal Aff., United States v. Nguyen, Cr. No. C-07-88, C.A. No. C-07-412 (S.D. Tex. Oct. 26, 2007); Harvey Rice, "Air Marshals Charged in Cocaine Smuggling Plot," *Houston Chronicle*, February 13, 2006, https://www.chron.com/news/houston-texas/article/Air-marshals-charged-in-cocaine-smuggling-plot-1897010.php.

[2] Andrew Becker, "Viagra-Smuggling Scandal Hits Federal Air Marshals," Yahoo, December 22, 2020, https://www.yahoo.com/now/viagrasmuggling-scandal-hits-federal-air-marshals-155928349.html.

[3] "Twelve Current and Former TSA and Airport Employees Indicted for Smuggling Approximately 20 Tons of Cocaine," 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.

suspect. Ultimately, six current and former TSA transportation security officers were found responsible for smuggling cocaine through the airport.[4]

In this thesis, an insider threat is the willful, malicious intent to cause harm to the flying public and damage TSA. Since the creation of TSA, insider threats have been identified on multiple occasions as one of the most significant dangers to the agency.[5] In February 2020, the Government Accountability Office (GAO) completed a report requested by Congress to assess TSA's Insider Threat Program. The report found that the threats include employees who damage aircraft and smuggle narcotics, weapons, and bulk cash.[6] Insider threats can affect various aspects of TSA's mission. Insider threats affect various aspects of TSA's mission and pose a problem specifically to its employees, aviation workers, and the flying public.

The conditions that give rise to insider threats are not static. A prime example is the impact of the COVID-19 pandemic on society. As COVID-19 spread across the country, many workplaces, including local, state, and federal government agencies, shifted their workforce from in-person to remote work. This shift has meant that many of the tools and processes for risk management designed for an in-office workforce are no longer enough to prevent insider threat activity.[7] Additionally, the pandemic has kept individuals in an extended state of high stress and uncertainty. As Michael Gelles, a known insider threat expert, points out, "Unusual times can provoke unusual responses in people. Prolonged stress may increase anxiety and impulsivity, impair judgment and lead people to become negative and distort their experiences. In times of crisis, individuals can begin to feel

[4] U.S. Attorney's Office, District of Puerto Rico.

[5] Transportation Security Administration, *Insider Threat Road Map 2020* (Springfield, VA: Transportation Security Administration, 2020), https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf.

[6] *TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals* (Washington, D.C.: Government Accountability Office, 2020), https://www.gao.gov/assets/gao-20-275.pdf.

[7] Karen A Toriello-Fite, "Insider Threat Risk Assessment and Telework" (Linthicum Heights, MD: Center for Development of Security Excellence, 2021), 18.

desperate, resulting in erratic behavior, potentially increasing the risk of insider events."[8] The pandemic has affected the way that work is done and how individuals perceive, interact with, and engage in society, potentially increasing the risk of insider threats. As the aforementioned incidents illustrate, existing procedures and protocols have shown only minimal success.

A. BACKGROUND

In 2013, TSA created an Insider Threat Program, which involved processes to curb insider threats, but the program has failed to fully detect and prevent them. Although TSA requires limited background checks and conducts randomized employee screenings, it lacks a strategic plan to guide its Insider Threat Program.[9] In 2015, TSA established an Insider Threat Advisory Group, a multi-office collective that reviews and analyzes activities, identifies gaps, and develops mitigation strategies.[10] However, the GAO warns that "TSA does not have a comprehensive set of performance goals that can be used to assess progress toward achieving the Insider Threat Program's stated mission."[11]

The Insider Threat Program's primary authority to operate lies with TSA's Law Enforcement Federal Air Marshal Service (FAMS). Along with the FAMS office, 22 additional TSA offices have responsibilities in the current program. These offices include security operations, multiple enrollment services, and vetting programs; inspection, investigations, intelligence, and analysis; and policy, plans, and engagement. This significant overlap increases the potential for duplicative effort and inefficiency.[12] TSA's program for proactive insider threat detection is threefold. It includes computer monitoring,

[8] Michael G. Gelles, "How to Handle the Risk of Insider Threats Post-COVID-19," TechTarget, May 12, 2020, https://searchcio.techtarget.com/feature/How-to-handle-the-risk-of-insider-threats-post-COVID-19.

[9] Triana McNeil, *Aviation Security: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals*, GAO-20-275 (Washington, DC: Government Accountability Office, 2020), https://www.gao.gov/products/GAO-20-275.

[10] McNeil.

[11] McNeil, 35.

[12] McNeil.

investigations of known allegations or whistleblower cases, and TSA Investigations' specialized Detect, Identify, Secure, and Counter (DISC) Program.

DISC originated in 2015 as a proactive effort to counter public corruption and mitigate the threat that criminal elements pose to TSA employees. DISC operations deploy a surge of TSA special agents to an unsuspecting airport and randomly select TSA employees for voluntary insider threat screening through polygraphs. Nevertheless, the Employee Polygraph Protection Act of 1988 helps to shield employees from being required to undergo polygraph examinations, and a genuine insider threat would likely decline to undergo any voluntary screening to avoid detection and arrest.[13] Therefore, having the investigative tools alone may not be effective if there is no requirement for all TSA employees to comply.

The outcomes of not having a robust and concise Insider Threat Program could lead to property destruction and harm to the traveling public. Implementing a more robust Insider Threat Program, however, may require significant expenditures and organizational culture change. Practices used by other agencies throughout the intelligence community have the potential to mitigate insider threats at TSA. Polygraphs, for example, have been a particularly effective tool and deterrent for employee misconduct in other agencies and have a good track record for identifying persons with hostile intentions against national security.[14]

As outlined in this section, TSA does not currently mandate a compulsory polygraph program for its employees, and all polygraphs require a specific purpose. TSA's management directives do not require employees to undergo polygraphs, and participation occurs only with an employee's consent. This thesis investigates whether and how TSA can benefit from adopting the previously vetted and utilized policies and procedures of other security-based organizations.

---

[13] Employee Polygraph Protection Act of 1988. Pub. L. No. 100–347, 102 Stat. 653 (1988), https://www.dol.gov/sites/dolgov/files/WHD/legacy/files/poly01.pdf.

[14] Vance MacLaren, "Can We Trust Counterintelligence Polygraph Tests?," *Polygraph* 29, no. 2 (2000): 151–54, https://www.polygraph.org/assets/docs/APA-Journal.Articles/Vol.29.2000/polygraph%202000%20292.pdf#page=16.

B. RESEARCH QUESTIONS

1. How can the TSA better address insider threats?
2. What policies and procedures do representative agencies in the United States and the United Kingdom use to address insider threats?
3. What are other organizations doing to mitigate insider threats?
4. Which policies and procedures may be of potential benefit to TSA?

C. RESEARCH DESIGN

This thesis explores how TSA can improve its defense against insider threats by assessing the policies and procedures of three organizations: the Department of Defense (DOD) and the Federal Bureau of Investigation (FBI) in the United States and the Centre for the Protection of National Infrastructure (CPNI) in the United Kingdom (UK). The two U.S. agencies are appropriate for study because they each screen broad types of personnel and have previous experiences with damaging insider threats. The UK, an American ally with similar laws, faces similar threats and maintains well-instituted insider threat programs. CPNI is the UK's premier authority on infrastructure protection, including insider threat detection and avoidance. This study describes how the FBI, DOD, and CPNI use continuous evaluation screening programs to mitigate insider threats, identifies policies and procedures that might benefit TSA, and identifies and assesses barriers and benefits to their adoption.

1. Agency and Critical Incident Selection and Data Sources

This thesis focuses on the FBI, DOD, and CPNI. Research for this thesis involved collecting data on the agencies and critical insider threat incidents that occurred for further analysis. The agencies selected for inclusion had to have security-sensitive missions and continuous evaluation insider threat programs in place. The information about the programs had to be publicly available. The selected agencies have maximized the breadth of tactics and solutions employed to mitigate insider threats and the variety of documented critical insider threat incidents.

The Department of Justice defines *critical incidents* as follows:

> Acts of terrorism, group defiance of governmental authority, hostage situations, and natural disasters. Typically, these events involve one or more of the following factors (although the presence of one factor by itself does not automatically mean that incident is critical):
>
> - Involves threats or acts of violence against government or social institutions.
> - Involves significant loss of life, significant injuries, or significant damage to property.
> - Demands use of substantial resources.
> - Attracts close public scrutiny through the media.
> - Requires coordination among federal law enforcement agencies (more so than usual), state or local law enforcement agencies, local or state prosecutors, emergency relief services, and/or emergency response services.
> - Requires ongoing communication with upper-level personnel at the Department of Justice.[15]

If any or all of the factors in this definition are met, the event is a critical incident. This thesis identifies two critical incidents per agency, with insiders representing a broad cross section of types of employment (e.g., contactor, civilian, and active duty). These attacks were significant enough to elicit agency case studies or public news articles. Identifying critical incidents and their details involved searching agencies' web pages and news outlets for reports.

This thesis relies on public sources of information published in the literature and by think tanks, the Department of Homeland Security, DOD, and CPNI in studies and reports. As TSA does not readily deal with classified information, this thesis utilizes primary sources, such as laws and policies, and secondary sources, such as books and scholarly articles.

Keyword searches were used to identify sources and critical incidents. The databases searched included Google Scholar, EBSCO, ProQuest, NewsBank, Dudley Knox Library, and the Homeland Security Digital Library. These searches resulted in a data set

[15] Eileen Regen Larence, *Information Sharing Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities*, GAO-13-471 (Washington, DC: Government Accountability Office, 2003), 1, https://www.ojp.gov/pdffiles1/Digitization/203371NCJRS.pdf.

of 276 documents including internal policy, news reports, regulations, laws, government audits, public records, and videos/webinars. The primary search terms included the following: insider threat AND FBI, DOD, CPNI, DOD technologies, England, UK, analysis, mitigation, continuous evaluation, incidents, and GAO report; employee screening AND polygraph, technology; DOD AND Robert Hanssen, insider threat program, Nidal Hassan, Navy Yard shooting; DITMAC; National Defense Authorization Act; UK data breach 2020; Hostile Reconnaissance; and FBI audit.

2. Data Analysis Approach

The analysis explored the organizational structure and culture of the focal organizations utilizing the Star model as a guiding framework. The Star model employs five categories of organization: strategy, structure, processes, reward systems, and human resource policies.[16] The analysis also used the additional category of technology. The Star model provides insight into how various strategies can lead to dissimilar establishments and why there is no universal organizational design for federal agencies.[17]

Next, the analysis identified each organization's mission, people, structure, processes, technologies, tactics, and solutions. The following questions guided the analysis: How do the selected agencies conduct their continuous evaluation; what programs, procedures, and technologies do they use; and what are the outcomes? This analysis utilized the following criteria to compare the selected agencies' continuous evaluation programs with that of TSA: whom they assess, assessment tactics used in screening, policies and technologies in place, strategic plans and critical incidents, and measures of effectiveness in detecting insider threats.

Finally, a timeline and case narrative were developed for each critical incident. The analysis assessed the role policy, procedures, and technologies played in explaining or influencing the outcomes of each incident and compared these factors across incidents to

[16] Jay Galbraith, "The Star Model," Galbraith Management Consultants, accessed May 11, 2021, https://www.jaygalbraith.com/images/pdfs/StarModel.pdf.

[17] Galbraith.

identify patterns. The analysis assessed the fit between potential solutions and TSA's organizational culture, structure, mission, and needs.

D. CHAPTER OUTLINE

Following this introduction, Chapter II reviews the existing literature. Chapter III describes TSA's current approach to insider threats. Chapter IV assesses the insider threat programs of the FBI, DOD, and CPNI, identifying policies and procedures that may benefit TSA and barriers and benefits to their adoption. Chapter V presents conclusions and recommendations.

II. LITERATURE REVIEW

The existing literature identifies and examines the effectiveness of various prevention tactics and solutions for insider threats to federal agencies.[18] While this literature shows that continuous evaluation (CE) effectively detects insider threats, studies of CE are limited. Although the literature suggests that many employee evaluation methods, such as background investigations and polygraphs, can reduce or prevent insider threats, findings show that the effectiveness of particular methods or a combination of evaluation methods varies. Researchers do not agree that one single method of vetting applicants and employees for insider threats is the most effective.[19] This review describes differing understandings of insider threats and their impacts; the process of CE; and contrasting assessments of the methods used for CE.

A. DEFINING AN INSIDER THREAT

There is no widely agreed-upon definition of an insider threat, but various government agencies have interpretations of what it constitutes.[20] Although agencies have defined the concept to align with their missions, their definitions are similar. All agencies define an insider threat as a person or group of persons that cause or intend to cause harm.

---

[18] MacLaren, "Can We Trust Counterintelligence Polygraph Tests?"; Steven Aftergood, "DOD Adds 'Credibility Assessment' to Polygraph Program," *Federation of American Scientists* (blog), February 12, 2007, https://fas.org/blogs/secrecy/2007/02/dod_adds_credibility_assessmen/; David Luckey et al., *Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Posture of the U.S. Departments and Agencies Be Improved?* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2684.html; Qussai Yaseen and Brajendra Panda, "Insider Threat Mitigation: Preventing Unauthorized Knowledge Acquisition," *International Journal of Information Security* 11, no. 4 (August 2012), http://dx.doi.org/10.1007/s10207-012-0165-6; Robert F. Mills, Gilbert L. Peterson, and Michael R. Grimaila, "Insider Threat Prevention, Detection and Mitigation," in *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*, ed. Kenneth J. Knapp (Hershey, PA: IGI Global, 2009), 48–74, https://www.igi-global.com/chapter/insider-threat-prevention-detection-mitigation/7410.

[19] Mills, Peterson, and Grimaila, "Insider Threat Prevention, Detection and Mitigation"; Sarah Young, "Continuous Evaluation: Background Investigations, Classified Information, and Informing in the 21st Century," Illinois Digital Environment for Access to Learning and Scholarship, March 15, 2019, https://doi.org/10.21900/iconf.2019.103373; Rita M. Barrios, "A Multi-Leveled Approach to Intrusion Detection and the Insider Threat," *Journal of Information Security* 4, no. 1 (2013): 54–65, https://doi.org/10.4236/jis.2013.41007; Transportation Security Administration, *Insider Threat Road Map 2020*.

[20] Luckey et al., *Assessing Continuous Evaluation Approaches for Insider Threats*, 2019.

Many definitions focus on foreign adversaries and counterintelligence.[21] Additionally, disclosing information is a key factor in most federal agency definitions. Interestingly, however, most agencies do not list violence as a factor. An agency's definition of an insider threat likely influences the mitigation strategies it employs, thus providing insight into the utility of particular strategies for TSA, given its mission. Table 1 displays the definitions of insider threat for the agencies included in this thesis. Understanding what constitutes insider threats is essential to developing strategies to identify and prevent them.

Table 1. Definitions of Insider Threat

Transportation Security Administration	"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."[22]
Department of Defense	"Insider threats are posed by employees or anyone else who has been granted trusted access to DOD information systems, installations, or facilities who commit a harmful act, intentional or not."[23]
Centre for the Protection of National Infrastructure	"A person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes. An insider could be a full time or part-time employee, a contractor or even a business partner. An insider could deliberately seek to join your organisation to conduct an insider act, or may be triggered to act at some point during their employment."[24]
Federal Bureau of Investigation	"Someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to any U.S. Government resource."[25]

[21] Luckey et al., xii.

[22] Department of Homeland Security, Office of Inspector General, *Transportation Security Administration Has Taken Steps to Address the Insider Threat but Challenges Remain*, OIG-12-120 (Washington, DC: Department of Homeland Security, Office of Inspector General, 2012), 2, https://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-120_Sep12.pdf.

[23] C. Todd Lopez, "DOD Program Aims to Deter Insiders from Harmful Acts," Department of Defense, September 17, 2019, https://www.defense.gov/Explore/News/Article/Article/1962031/dod-program-aims-to-deter-insiders-from-harmful-acts/.

[24] "Reducing Insider Risk," Centre for the Protection of National Infrastructure, May 25, 2021, https://www.cpni.gov.uk/reducing-insider-risk.

[25] Department of Justice, Office of the Inspector General, *Public Summary: Audit of the Federal Bureau of Investigation's Insider Threat Program* (Washington, DC: Department of Justice, Office of the Inspector General, 2017), 2, https://sgp.fas.org/othergov/dojig-itp.pdf.

Researchers have also suggested that characteristics not included in the definitions of insider threat above may contribute to an organization's ability to identify a threat. For example, changing existing behavior or engaging in a new behavior can indicate a potential insider threat. In their simulation, Taylor et al. found that day-to-day work behavior, such as becoming more self-focused and shifting language patterns, may be affected as a person considers or carries out an attack.[26] This research comports with Caputo, Maloof, and Stephens's assessment that "of the employees whose behavior differed from the norm, 84% were carrying out insider attacks."[27] Some researchers have, thus, argued that the definition of insider threat needs to be more nuanced. For example, Luckey et al. further break down the definition of insider threat by the type of insider: the traitor, the zealot, the browser, the well-intentioned, and the violent insider.[28] This sort of classification moves toward a more systematic scoping of what threats may exist now and in the future.[29]

In this thesis, an insider threat is defined as one or more individuals with access or inside knowledge that, wittingly or unwittingly, allows them to exploit the security vulnerabilities of the United States and cause harm. This definition combines several key aspects of the identified definitions above. For example, that a threat may consist of multiple individuals is important based on TSA's experience with smuggling rings. Additionally, this definition includes malicious and unintentional acts. Last, harmful outcomes are not explicitly stated as this thesis examines the insider threat within multiple agencies, and what constitutes "harm" may differ.

B. INCREASED VULNERABILITY TO INSIDER THREATS

Numerous experts claim that not only is insider threat an issue, but the United States is experiencing greater vulnerability to these threats partly due to its status as a dominant

[26] Paul J. Taylor et al., "Detecting Insider Threats through Language Change," *Law and Human Behavior* 37, no. 4 (August 2013): 267, http://doi.org/10.1037/lhb0000032.

[27] Taylor et al., 267.

[28] Luckey et al., *Assessing Continuous Evaluation Approaches for Insider Threats*, 2019.

[29] Luckey et al., xi.

force in an increasingly aggressive global economy.[30] Figure 1 highlights several of the factors contributing to growing vulnerabilities to insider threats. As a result of the United States' dominant position in a competitive global economy, along with difficulties associated with controlling access to emerging technologies, foreign demand for protected information is increasing.[31] According to Kramer and Heuer, "The need to protect U.S. information is critical and vital to protect our homeland. The increasing dependence upon networked databases exponentially increases the amount of information a single malicious insider can access."[32] Additionally, the prevalence of international travel increases opportunities for foreign entities to gain access to protected information.[33] Reducing insider threats within the government and private infrastructure is a homeland security imperative. This vulnerability, if not mitigated, could have significant dire effects on the homeland and its essential services.

[30] McNeil, *TSA Could Strengthen Its Insider Threat Program*, 1.

[31] Lisa A. Kramer and Richards J. Heuer Jr., "America's Increased Vulnerability to Insider Espionage," *International Journal of Intelligence and CounterIntelligence* 20, no. 1 (2007): 50, https://doi.org/10.1080/08850600600888698.

[32] Kramer and Heuer, 50.

[33] Kramer and Heuer, 50.

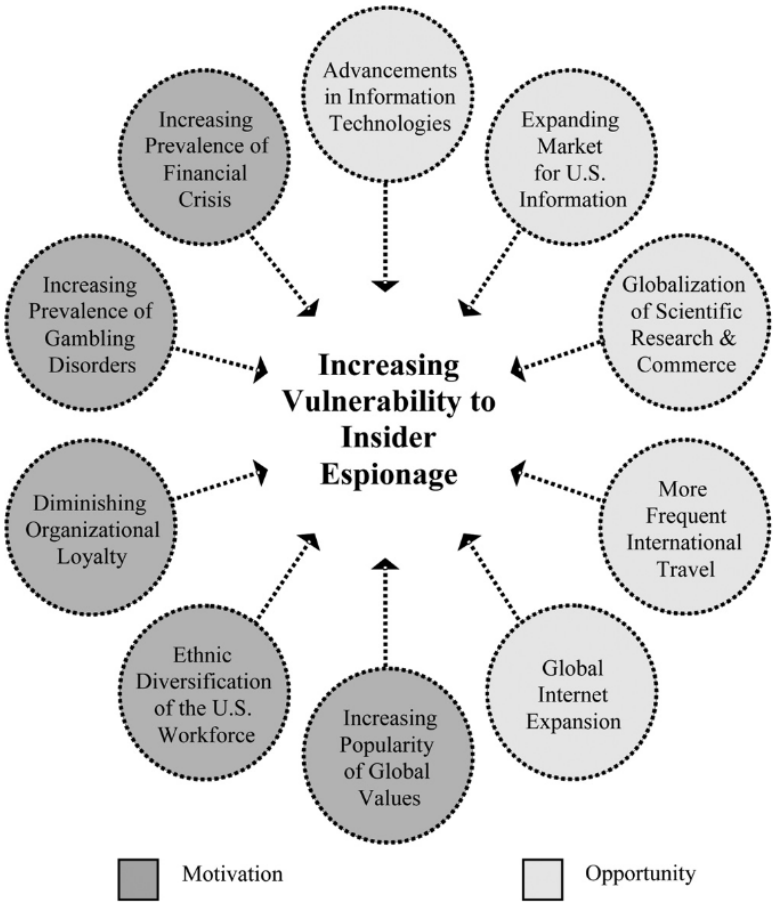

Figure 1. Factors Contributing to Increasing Vulnerability.[34]

C. SCOPING THE PROBLEM

Numerous authors and experts concur that for TSA, an increase in vulnerability is especially worrisome as many parts of transportation infrastructure are susceptible to insider threats. The GAO cited numerous incidents of aviation workers using their provable access to smuggle contraband onto planes and into secure areas.[35] TSA bears the main responsibility of protecting airports around the country.[36] Transportation infrastructure and

[34] Source: Kramer and Heuer, 58.

[35] Jennifer Grover, *Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates*, GAO-16-632 (Washington, DC: Government Accountability Office, 2016), https://www.gao.gov/products/gao-16-632.

[36] Grover.

the organizations that secure the transportation sector rely heavily on data and digital technologies. The transportation sector along with other critical infrastructure is highly susceptible to internal and external cyberattacks. Bad actors or insider threats understand the value and vulnerabilities of the transportation sector and have the potential to cause widespread harm with little effort.[37] Indeed, as Martin Ruder claims in an article for the *International Journal of Intelligence and CounterIntelligence*,

> Infrastructure sectors and institutions in various jurisdictions that are known to have experienced insider threats from international jihadist elements in recent years include airports, airlines, energy utilities, nuclear plants, petroleum companies, university laboratories, water systems, sensitive government departments, and security agencies in Denmark, the Netherlands, the UK, and the U.S.[38]

When it comes to the transportation sector, experts have voiced significant concerns about increasing threats specifically to air transportation by airport employees, including TSA agents, airport shop employees, refuelers, and baggage handlers, who have been pitched by known terrorists.[39] Between 2020 and 2021, there was a significant rise in actionable insider threat incidents, but not every threat was violent in nature; a portion of those insider threat actions involved data theft, whose most likely victims were government agencies.[40] With over 50,000 employees, the likelihood that TSA will experience a significant insider threat event is high.

D. IMPACTS OF INSIDER THREATS

The cost of insider threats can be tangible or intangible.[41] Robert Hanssen, for example, slipped through his reinvestigation process and caused harm to the United

---

[37] Martin Rudner, "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge," *International Journal of Intelligence and CounterIntelligence* 26, no. 3 (September 2013): 453–81, https://doi.org/10.1080/08850607.2013.780552.

[38] Rudner, 469.

[39] Rudner, 469.

[40] "Insider Threats: Why These Cybersecurity Incidents Continue to Grow," Dice, February 21, 2022, https://www.dice.com/career-advice/insider-threats-why-these-cybersecurity-incidents-continue-to-grow.

[41] Luckey et al., *Assessing Continuous Evaluation Approaches for Insider Threats*.

States.[42] Hanssen impaired diplomacy and intelligence gathering, causing estimated monetary damages of approximately $25–$35 billion to the cloud-computing industry from the industry and proprietary secrets he leaked.[43] These leaked secrets resulted in distrust of and lost business for U.S.-based companies due to concerns that the United States had been spying on customers.[44] One insider threat can inflict significant damage to an organization. Notably, the actions of former FBI agent and Russian spy Robert Hanssen resulted in what has been described as the worst intelligence disaster in U.S. history.[45] Hanssen's actions demonstrate the substantial cost that can be incurred when an employee misuses one's organizational access and information. While a total estimate has not been publicly disclosed, some estimate that between 1985 and 1991, the U.S intelligence programs experienced hundreds of millions of dollars of damage due to Hanssen's espionage.[46] The impacts of Hanssen's betrayal were not only financial, as at least three human assets were killed.

As demonstrated by the Hanssen example, the full breadth and magnitude of impacts are often unknown. According to Luckey et al., "U.S. department and agency data and the physical security of personnel employed by the United States and those who conduct business at or visit U.S. facilities are at risk from this threat. The costs due to the erosion of confidence by U.S. employees, the U.S. population, and U.S. allies are also significant."[47] The tangible and intangible consequences can be dire, tragic, and embarrassing to the U.S. government.

---

[42] Sarah Young, "Slipping through the Cracks: Background Investigations after Snowden," *Surveillance & Society* 15, no. 1 (2017): 123–36, https://doi.org/10.24908/ss.v15i1.5306.

[43] Sune von Solms and Renier van Heerden, "The Consequences of Edward Snowden NSA Related Information Disclosures," in *Proceedings of the 10th International Conference on Cyber Warfare and Security* (Reading, UK: Academic Conferences and Publishing International, 2015).

[44] von Solms and van Heerden.

[45] E. Eugene Schultz, "A Framework for Understanding and Predicting Insider Attacks," *Computers & Security* 21, no. 6 (2002): 526–31, https://doi.org/10.1016/S0167-4048(02)01009-X.

[46] "A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen," Department of Justice, Office of the Inspector General, August 14, 2003, https://irp.fas.org/agency/doj/oig/hanssen.html.

[47] Luckey et al., *Assessing Continuous Evaluation Approaches for Insider Threats*, ix.

E. CONTINUOUS EVALUATION

Although the U.S. government has a definition for CE in practice, the process is relatively new and has not been defined more permanently in federal statutes.[48] The Obama administration established a definition of CE for the executive branch of the federal government in Executive Order 13764. According to this definition, CE is "a vetting process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility."[49]

The U.S. Intelligence Community uses the CE method employed by the Office of the Director of National Intelligence (ODNI), which establishes eligibility standards for access to sensitive or controlled information.[50] Furthermore, Intelligence Community (IC) Directive 704 declares, "All IC security elements shall accept in-scope personnel security investigations and access eligibility determinations that are void conditions, deviations or waivers."[51] That directive establishes and legitimizes CE. However, as Luckey et al. explain, "Many CE programs, particularly within the government, remain in the early phases and are not yet fully operational. The effectiveness of these programs remains somewhat obscure, as most results are not yet publicly available, and it could take time to realize measurable benefits and assess success."[52]

Understanding existing program effectiveness and performance measures is vital to organizations that need to screen for insider threats. One possible method for evaluating CE programs would be to utilize the standards set by the Defense Personnel and Security Research Center (PERSEREC) to assess the efficacy of personnel security programs within

---

[48] Luckey et al., 7.

[49] Exec. Order No. 13764, 82 Fed. Reg. 8115 (January 23, 2017), https://www.hsdl.org/?abstract&did=798174.

[50] Office of the Director of National Intelligence, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*, ICD 704 (Washington, DC: Office of the Director of National Intelligence, 2008), https://www.hsdl.org/?abstract&did=234672.

[51] Office of the Director of National Intelligence, 2.

[52] Luckey et al., *Assessing Continuous Evaluation Approaches for Insider Threats*, xi.

the federal government. First, the program's objectives and performance criteria must be established to evaluate performance properly.[53] The PERSEREC program's performance criteria for evaluation are as follows:

- Timeliness (refers to operational deadlines for completing an objective)
- Efficiency (refers to resources expended to accomplish an objective)
- Fairness (refers to legal and appropriate treatment of program participants).[54]

1. Benefits of CE

Experts argue the CE process offers numerous benefits. In an exploratory report, Luckey et al. suggest one potential benefit of CE and screening is that "individuals are reviewed in near-real time" and that constant attention can "reduce the actual costs associated with the security clearance and suitability/fitness vetting processes."[55] In addition to the potential benefits of detecting insider threats, organizations may experience other efficiencies. For example, CE employs much of the same information used in existing investigation and reinvestigation practices; the data are simply utilized more frequently.[56]

CE relies on identifying and integrating both behavioral and cyber indicators. While data related to human factors are not as readily obtained or assessed as technological indicators, they are essential for more proactive programs.[57] This proactive monitoring aids in identifying motivations and contributing factors related to insider behavior, giving the organization an opportunity to address them before an attack occurs.[58]

---

[53] Eric L. Lang, *Security Background Investigations and Clearance Procedures of the Federal Government*, Management Report 05–5 (Monterey, CA: Defense Personnel and Security Research Center, 2005), x, https://www.dhra.mil/Portals/52/Documents/perserec/mr05-05.pdf.

[54] Lang, x.

[55] Luckey et al., *Assessing Continuous Evaluation Approaches for Insider Threats*, x.

[56] Luckey et al.

[57] Frank L. Greitzer, "Insider Threats: It's the Human, Stupid!," in *Proceedings of the Northwest Cybersecurity Symposium* (New York: Association for Computing Machinery, 2019), 1–8, https://doi.org/10.1145/3332448.3332458.

[58] Greitzer.

2. Challenges for Implementation

A lack of publicly available information and literature on actual insider threats limits CE and its methods. Luckey et al. contend, "There are limited behavioral or technical data available to develop and deploy an effective and predictive CE monitoring tool. Scholars and practitioners of CE have been forced to develop technical solutions based on generalized behavioral indicators because access to actual insider threats and their associated data streams is not available."[59]

Experts claim that employee screening programs are not perfect, and the extra screening and evaluation measures associated with CE programs will increase work and the administrative load. Given the sizable backlog in clearance processing, agencies would need to determine whether they have the capacity to implement CE procedures.[60] Charles Phalen, director of the National Background Investigations Bureau, testified before the House Oversight and Government Reform Committee about the factors contributing to the nearly 10-year backlog—the Office of Personnel Management's losing its largest contractor, a major cybersecurity hack, and the 2012 Federal Investigative Standards implementation, which dramatically altered the background investigation requirements.[61] Experts at the International Air Transportation Association recommend performing a pre-screening with a background check, arguing that the standard policy is to hire only applicants who provide personal information and meet the organization's suitability requirements for access to sensitive areas at the airport.[62] Considering the costs and benefits of CE programs, additional research on this topic is warranted.

---

[59] Luckey et al., *Assessing Continuous Evaluation Approaches for Insider Threats*, xiii.

[60] Luckey et al., 2.

[61] Charles Phalen, "Statement before the Subcommittee on Government Operations, House Oversight and Government Reform Committee, United States House of Representatives" (Washington, DC: Office of Personnel Management, 2017), https://www.opm.gov/news/testimony/115th-congress/nbib-director-charles-phalen-testimony-before-hogr-govt-operations-subcommittee.pdf.

[62] International Air Transportation Association, *Insider Threat in Civil Aviation* (Montreal: International Air Transportation Association, 2018), 2, https://www.iata.org/contentassets/e55ae27b2fc34343a1143fca5129c8dd/insider-threats-position.pdf.

CE raises privacy concerns and counterarguments about whether the benefits outweigh the downsides. Some argue that CE may be less invasive to the previously vetted population.[63] Others argue that CE is an invasion of the government employee's privacy. For example, Ebersole claims that CE "creates a complete picture of an individual that invades every relationship, belief, and sanctuary to an extent that precludes privacy."[64] It is safe to say there is no consensus on this point.

3. CE Methods

Authors have explored multiple methods for conducting CE, including polygraphs, background investigations, ocular-motor deception tests, psychological evaluations, financial and credit screening, social media screening, risk assessment, and screening interviews. While these evaluation methods alone cannot defeat or prevent all insider threats, experts claim that utilizing an ongoing, multifaceted approach could be helpful in the fight against insider threats. The following subsections detail these methods.

a. Policies and Procedures for Assessment

Literature has supported the use of polygraph examinations as part of the screening process for federal agencies. In a literature review of all aspects of polygraph testing procedures, Nelson found that "results from several decades of scientific study have consistently supported the validity of the hypothesis that the combination of instrumental recording and statistical modeling can discriminate deception and truth-telling at rates significantly greater than chance"—thus confirming the value of these methods to any CE program.[65] In an open-source literature review of the polygraph screening practices used by the DOD, MacLaren concurs with Nelson and adds that polygraph screening practices play a valuable role in maintaining national security.[66] IC Directive 704 further articulates that the polygraph is a viable tool in CE. As seen with the IC, polygraph examinations may

---

[63] Luckey et al., *Assessing Continuous Evaluation Approaches for Insider Threats*, x.

[64] Kyle Ebersole, "Continuous Evaluation: Welcoming Government Employees to the World of Mass Surveillance," *George Mason Law Review* 23, no. 2 (2016): 445–77.

[65] Raymond Nelson, "Scientific Basis for Polygraph Testing," *Polygraph* 44, no. 1 (2015): 42.

[66] MacLaren, "Can We Trust Counterintelligence Polygraph Tests?"

be required "when the Head of an IC Element deems it to be in the interest of national security."[67]

However, there are concerns about the ethics of polygraph testing. Nelson warns, "Because polygraph tests—like all tests—are inherently probabilistic (i.e., they are neither deterministic observation nor physical measurement), they are not perfect."[68] Even the backers of polygraphs warn of their inherent limitations, so they advise that these tests not be used as the stand-alone method for CE.[69]

Psychological evaluations are a relatively standard part of the clearance investigation process.[70] In one report, PERSEREC assesses whether insider attacks could be prevented by including all DOD applicants in a psychological screening.[71] In another, PERSEREC's subject-matter experts recommend that training for conducting CE psychological evaluations should familiarize clinicians with the concept of insider threats and the potential risks of granting clearance to someone who exhibits poor judgment, reliability, or trustworthiness.[72] Other subject-matter experts have also recommended expanding psychological screening to more applicants.[73]

Psychological evaluations are not without some complications, however. Writing for PERSEREC, Baweja et al. maintain,

> First, psychological assessments require significant resources and, thus, are expensive. Psychological assessments also present an opportunity for

---

67 Office of the Director of National Intelligence, *Personnel Security Standards and Procedures*, 2.

68 Nelson, "Scientific Basis for Polygraph Testing," 44.

69 Sandra N. Hurd, "Use of the Polygraph in Screening Job Applicants," *American Business Law Journal* 22, no. 4 (Winter 1985): 529–49, ProQuest.

70 Scott Edwards, "The Psychological Evaluation and Your Security Clearance: Why You Shouldn't Overshare," Clearance Jobs, November 22, 2020, https://news.clearancejobs.com/2020/11/22/the-psychological-evaluation-and-your-security-clearance-oversharing-can-ruin-your-career/.

71 Jessica A. Baweja et al., *An Evaluation of the Utility of Expanding Psychological Screening to Prevent Insider Attacks*, OPA Report No. 2019–067 (Seaside, CA: Defense Personnel and Security Research Center, Office of People Analytics, 2019), https://apps.dtic.mil/sti/citations/AD1083812.

72 Kristin G. Schneider et al., *A Personnel Security Training Program for Clinicians: Phase III*, OPA Report No. 2020–002 (Seaside, CA: Defense Personnel and Security Research Center, Office of People Analytics, 2019), 20, https://apps.dtic.mil/sti/citations/AD1089287.

73 Baweja et al., "Expanding Psychological Screening to Prevent Insider Attacks."

> applicants to misrepresent themselves in an effort to get hired, which must be accounted for in screening programs . . . . Finally, screening programs may have consequences (e.g., decreased morale or recruitment), so organizations should consider the benefits relative to risk prior to implementation.[74]

Organizations face the difficult tasks of maintaining a balance between security and employee morale and retaining personnel.

b. Screening Methods

Screening potential employees in the private sector is typically done to assess an applicant's potential for success within the organization. For some federal organizations, applicant and employee screening can also be used to determine whether the applicant may threaten the organization. This vetting for the clearance process may include background checks, interviews, identity verification, a personal history, and a review of work history.[75] This verification can include basic information such as one's home address, social media activity, credit reports, mental health verification, and criminal records checks.[76]

Background investigations are another CE method. Young explains, "Investigators conducting [background investigations] gather information from those that want security clearances, and government officials use the information to sort those under investigation into threat classification levels."[77] According to the Center for Development of Security Excellence, "CE modernizes the background investigation process by maximizing automated records checks to identify adjudicative relevant information to assist in assessing the continued eligibility of individuals at any time during their period of eligibility."[78] Studies on the effectiveness of background investigations are limited, and a

---

[74] Baweja et al., 6.

[75] ASIS International, *Risk Assessment*, vol. 1 (Alexandria, VA: ASIS International, 2015), http://www.asisonline.org/publications--resources/standards--guidelines/ra/annex-c/.

[76] ASIS International, 1:1.

[77] Young, "Continuous Evaluation," 1.

[78] Center for Development of Security Excellence, *Introduction to Personnel Security: Student Guide*, PS113.16 (Linthicum Heights, MD: Center for Development of Security Excellence, 2020), 6, https://www.cdse.edu/documents/student-guides/PS113-guide.pdf.

background investigation may be insufficient to properly and completely vet an individual in a high-level position. In his NPS thesis, Hill argues that the financial backgrounds of employees with top-secret security clearances should play a larger role in the vetting process.[79] Financial information is a factor commonly included in background investigations. Background investigations and periodic reinvestigations address other suitability factors such as substance abuse, excessive gambling issues, criminal history, financial delinquencies, mental health problems, and obligations to or influences of non-U.S. citizens or those disloyal to the United States.[80]

Federal employers can conduct a criminal records check for applicants. These checks gather information about a person's criminal history, if any. These records are obtained from criminal justice agencies such as local police departments, courts, and the FBI's offender registry lists. The information that employers can obtain in a records check includes local, state, or federal arrests and any form of detention, such as jail or prison time served. Records checks can also include traffic offenses, indictments, criminal charges, detentions without charges, and dispositions from charges. Finally, any fines assessed for criminal charges are typically indicated in the records.[81]

The cost-effective method of criminal history checks can benefit an agency by preventing and reducing insider threats. Candidates with criminal histories exhibit a higher risk of future criminal behavior than applicants who have no criminal background.[82] The relatively low cost of criminal records checks is ideal for protecting the workforce. Some have argued against the use of criminal record checks. For example, criminal records checks might falsely identify an applicant as a person with a criminal history or fail to

[79] Henry J. Hill, "Impact of Altering the Delinquent Debt Threshold Used for Background Investigation Expansion on the Denial Rate of Security Clearances" (master's thesis, Naval Postgraduate School, 1991), https://apps.dtic.mil/sti/pdfs/ADA247331.pdf.

[80] Kramer and Heuer, "America's Increased Vulnerability to Insider Espionage," 50.

[81] "What Is a Criminal Record Check?," Workplace Testing, May 29, 2020, http://www.workplacetesting.com/definition/710/criminal-record-check.

[82] Megan C. Kurlychek, Robert Brame, and Shawn D. Bushway, "Enduring Risk? Old Criminal Records and Predictions of Future Criminal Involvement," *Crime & Delinquency* 53, no. 1 (2007): 64–83, https://doi.org/10.1177/0011128706294439.

adequately capture someone's criminal background.[83] Moreover, there is an overall bias against people with criminal histories even though a portion of applicants with a criminal past may not pose an insider threat.

Insider threats commonly experience financial issues or are motivated by money or gifts to betray their organization or country. Kramer advises that a financial crisis can be a critical factor in creating or increasing a person's motivation to spy.[84] In 2001, the FBI arrested Brian Regan, a U.S. Air Force intelligence analyst, for stealing classified materials with the intention of selling them to foreign adversaries. Regan possessed over $100,000 in credit card debt during the investigation.[85] Regan is a prime example of the power of personal financial distress in spurring espionage.[86] Monitoring the financials and credit of employees can provide key information on undue affluence or significant debt. One technology that currently exists involves a financial triggers program, which continuously monitors credit risk for individuals. The federal government could leverage this technology to gauge the financial health of its employees, monitoring large debt accrual in a short period, late payments on financial obligations such as loans, or procurement of additional loans or mortgages outside employees' means.[87]

However, a hurdle that federal agencies may encounter is the Fair Credit Reporting Act, which provides protections to individuals regarding the information provided by consumer reporting agencies to employers.[88] The standard federal background investigation asks that applicants consent to credit report monitoring. Hill points out in his NPS thesis that financial screening, such as identifying delinquent debt levels, is a poor

83 "Five Problems with Criminal Background Checks," Urban Institute, accessed June 12, 2022, https://www.urban.org/urban-wire/five-problems-criminal-background-checks.

84 Kramer and Heuer, "America's Increased Vulnerability to Insider Espionage."

85 "Brian P. Regan Espionage," Federal Bureau of Investigation, accessed June 6, 2022, https://www.fbi.gov/history/famous-cases/brian-p-regan-espionage.

86 Kramer and Heuer, "America's Increased Vulnerability to Insider Espionage."

87 Bryan Denson, "How Financial Triggers Can Help Spot Insider Threats," GCN, August 5, 2020, https://gcn.com/cybersecurity/2020/08/how-financial-triggers-can-help-spot-insider-threats/315135/.

88 Fair Credit Reporting Act, 15 U.S.C. § 1681 (2022), http://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

indicator of employment suitability or determiner of final clearance outcomes.[89] Overall, the amount of relevant information obtained from credit checks for the relatively low cost of credit monitoring makes this method highly appealing.[90] Even though this simple, inexpensive screening measure is not perfect, it can still benefit organizations.

Social media is a digital channel where participants can create and share information. Social media members can include their personal data, photos, and videos on social media platforms, which can be accessed by the general public or a select audience. Federal government organizations can monitor and utilize applicants' and employees' social media accounts in security background checks, gleaning such information as individuals' associations with organizations or other individuals. Investigators can determine behaviors and conduct related to the predetermined guidelines for the background investigation.[91] However, the ODNI has determined that "the period of coverage for publicly available electronic information will be consistent with the scope of the investigation."[92] Employers may search for inflammatory or derogatory statements or photos or videos of inappropriate behavior. Such social media posts could be solid indicators of potential liabilities or insider threats to the hiring organization.[93] Nevertheless, while Sweeny argues in his thesis that social media screening for applicants could infringe on free speech rights, it is cost-effective method for screening.[94]

Interviews are conversations between employers and employees or applicants. The interview methods can vary, from individual to panel interviews. These interviews, either free flowing or structured, can be used to prevent or greatly reduce the chance of an insider threat. Management can utilize interviews as an intervention technique for employees

89 Hill, "Delinquent Debt Threshold."

90 Lang, *Security Background Investigations*.

91 Office of the Director of National Intelligence, *Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications*, SEAD-5 (Washington, DC: Office of the Director of National Intelligence, 2016), 3, https://www.cdse.edu/documents/toolkits-personnel/SEAD-5.pdf.

92 Office of the Director of National Intelligence, 3.

93 Denis Sweeney, "Social Media Screening of Homeland Security Job Applicants and the Implications on Free Speech Rights" (master's thesis, Naval Postgraduate School, 2019).

94 Sweeney.

suffering personal problems or employment issues because they can escalate into a security risk, such as workplace violence or espionage.[95] This simple, low-technology technique can provide a significant safeguard for the workforce.

Another less-invasive CE technique is the ocular-motor deception test (ODT). As Jacobs and Dell'Osso explain, this test "leverages the changes in a person's pupil's size over a series of questions to determine truth or deception."[96] This technology assumes "that lying is cognitively more demanding than telling the truth."[97] Through a series of laboratory and field studies, Kircher and Raskin, former proponents of the polygraph, found that "ODT yields accuracy greater than 80% on both truthful and deceptive examinees."[98] Furthermore, Kircher and Raskin found that the ODT is effective with people who cannot read well.[99] Since the technology is relatively new, no studies or attempts to investigate possible countermeasures to defeat the ODT have been undertaken.[100]

Information technology (IT) is ubiquitous in all workplaces. IT stores valuable information and enables communication in a secure fashion. However, insiders have no need to bypass the inherent extra-security features present in IT services as they already have permission to access the organization's systems and information. An insider threat detection system (ITDS) can operate via passive automated monitoring of employee behavior on an organization's internal IT system.[101] While most commercial ITDS systems are marketed toward larger organizations, an increasing number of lower-cost

---

95 Kramer and Heuer, "America's Increased Vulnerability to Insider Espionage."

96 Jonathan B. Jacobs and Louis F. Dell'Osso, "Congenital Nystagmus: Hypotheses for Its Genesis and Complex Waveforms within a Behavioral Ocular Motor System Model," *Journal of Vision* 4, no. 7 (July 2004): 604, https://doi.org/10.1167/4.7.7.

97 John Kircher and David Raskin, "Laboratory and Field Research on the Ocular-Motor Deception Test," *European Polygraph* 10, no. 4 (2016): 160, https://doi.org/10.1515/ep-2016-0021.

98 Kircher and Raskin, 169.

99 Kircher and Raskin.

100 Kircher and Raskin.

101 Shannon Wasko et al., "Using Alternate Reality Games to Find a Needle in a Haystack: An Approach for Testing Insider Threat Detection Methods," *Computers & Security* 107 (2021), https://doi.org/10.1016/j.cose.2021.102314.

options have come to market to break down the barriers and cost of entry.[102] Another challenge of passive methods is the massive quantity of alerts produced during monitoring and the vast resources to investigate them all, especially since the majority are likely to be false positives and not true threats.[103] To address this inherent issue, researchers have begun to develop and test active indicators that, when inserted into standard organizational workflows, instigate different behaviors in insider treats compared to nonthreatening employees. According to Wasko et al., "An example of an active indicator could be an email announcement that a hard drive scan will be taking place on employees' computers. Whereas typical employees may not make an overt response to the announcement, those who were acting maliciously may try to conceal their activities by deleting files, deleting software, or taking similar actions."[104]

In addition to cost and time intensiveness, there are a few other challenges associated with monitoring IT. Due to privacy concerns, most organizations do not disclose actual insider threat data, making it difficult to develop and test an ITDS.[105] These tools are also often static, so it can be difficult for them to adapt as insider threat behavior advances over time. For example, insiders may use technology, such as cryptography, to mask their exploits or slowly evolve their tactics to subvert timed data strategies and static policies.[106] Last, most IT screening systems are designed to track an individual's behavior, making it difficult to detect a collaborative attack conducted by multiple insiders.[107]

---

[102] Derrick Spooner et al., "Navigating the Insider Threat Tool Landscape: Low Cost Technical Solutions to Jump Start an Insider Threat Program," in *2018 IEEE Security and Privacy Workshops* (Piscataway, NJ: IEEE, 2018), 247–57, https://doi.org/10.1109/SPW.2018.00040.

[103] Yulia Cherdantseva et al., "A Review of Cyber Security Risk Assessment Methods for SCADA Systems," *Computers & Security* 56 (February 2016): 1–27, https://doi.org/10.1016/j.cose.2015.09.009; Wasko et al., "Using Alternate Reality Games to Find a Needle in a Haystack"; Mohammed Nasser Al-Mhiqani et al., "A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations," *Applied Sciences* 10, no. 15 (January 2020): 5208, https://doi.org/10.3390/app10155208.

[104] Wasko et al., "Using Alternate Reality Games to Find a Needle in a Haystack."

[105] Al-Mhiqani et al., "A Review of Insider Threat Detection."

[106] Al-Mhiqani et al.

[107] Al-Mhiqani et al.

F. CONCLUSION

While gaps exist in the literature around detecting insider threats and performing CE, the literature recognizes the increased risk of insider threat activity and multiple methods under development or currently employed to prevent attacks proactively or minimize their impact. The next two chapters explore how these methods are operationalized into comprehensive insider threat programs.

THIS PAGE INTENTIONALLY LEFT BLANK

III. TSA'S INSIDER THREAT PROGRAM

In 2001, Congress passed the Aviation and Transportation Security Act, which created TSA and tasked it with securing the aviation, maritime, mass transit, highway, and freight rail transportation pipelines.[108] TSA plays a critical role in most Americans' lives by allowing people and commerce to move freely and securely and by protecting transportation sectors.[109] For the Americans who use transportation infrastructure, TSA fulfills a critical role in securing those channels. TSA employs approximately 60,000 employees including 50,000 transportation security officers and 600 aviation transportation security inspectors, transportation security specialists, FAMs, and other security personnel. Much of TSA's effort is spent securing air travel in the 440 federalized airports around the country and screening approximately 750 million passengers annually. Another major component comprises FAMs, armed federal law enforcement agents who fly clandestinely on commercial passenger aircraft to protect the passengers and airline crew from criminal and terror threats. FAMs also openly protect ground transportation, such as train stations and metro centers, along with local law enforcement.[110] This chapter briefly examines TSA's insider threat issues; dives into TSA's employee screening methods, policies, procedures, and technologies used to combat insider threats; and concludes with some key findings.

A. HOW INSIDER THREATS IMPACT TSA

TSA and transportation sector employees can be a risk to TSA, and American lives hang in the balance. From TSA's perspective, an insider threat is the willful, malicious intent to cause harm to the flying public and damage the airline industry.[111] The incidents

[108] Aviation and Transportation Security Act, Pub. L. No. 107–71, 115 Stat. 597 (2001), https://www.congress.gov/107/plaws/publ71/PLAW-107publ71.pdf.

[109] "Mission," Transportation Security Administration," accessed January 30, 2022, https://www.tsa.gov/about/tsa-mission.

[110] "Law Enforcement," Transportation Security Administration, accessed January 31, 2022, https://jobs.tsa.gov/law-enforcement.

[111] McNeil, *TSA Could Strengthen Its Insider Threat Program*.

described in the previous chapters exemplify a more significant problem. Insider threats include TSA, airport, and airline employees who damage aircraft and smuggle narcotics, weapons, and bulk cash. The Department of Homeland Security (DHS) and TSA have specifically requested funds to address insider threats to the latter and the transportation sector. For fiscal year 2022, TSA was allotted $27.2 million, and 334 full-time employees were detailed specifically to its Insider Threat Program (ITP).[112] However, for fiscal year 2023, TSA has funded this program through technology development in the research and development budget.[113] The struggle to dedicate funds consistently to insider threat deterrence is constant.

A significant portion of the transportation sector is privately owned. There are no federal mandates for the private sector to have an ITP let alone critical infrastructure.[114] However, TSA works with the private sector to help secure its transportation modalities with various tools and resources.[115]

B. SCREENING

All prospective TSA applicants submit an application, and selectees are interviewed by a hiring official. For TSA jobs that require a security clearance, the applicant must be granted the clearance before being offered the position. For other TSA positions, applicants must pass a computer-based evaluation to move forward in the hiring process. There are different levels of screening for sworn law enforcement as they also

112 Department of Homeland Security, *FY 2022 Budget in Brief* (Washington, DC: Department of Homeland Security, 2021), 46, https://www.dhs.gov/sites/default/files/publications/dhs_bib_-_web_version_-_final_508.pdf.

113 Department of Homeland Security, *Transportation Security Administration Budget Overview: Fiscal Year 2023 Congressional Justification* (Washington, DC: Department of Homeland Security, 2022), 313, https://www.dhs.gov/sites/default/files/2022-03/Transportation%20Security%20Administration_Remediated.pdf.

114 Intelligence and National Security Alliance, Insider Threat Task Force, *A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector* (Arlington, VA: Intelligence and National Security Alliance, 2013).

115 "For Industry," Transportation Security Administration," accessed January 13, 2022, https://www.tsa.gov/for-industry.

require a pre-employment polygraph.[116] However, once an applicant is selected and hired, TSA does not conduct additional or continuous evaluations on employees. TSA employees with a clearance are the exception as they need periodic background reinvestigations to maintain their high-level clearance.

Table 2. TSA Applicant Requirements.[117]

Requirements	Law Enforcement	Executives	Mission Support	Security
At least 18 years old*	X	X	X	X
U.S. citizenship	X	X	X	X
High school education	X			X
Four-year degree		X	X	
Background investigation	X	X	X	X
Pre-employment drug test	X	X	X	X
Computer-based test (evaluation)				X
Medical evaluation	X			X
Polygraph	X			
Financial disclosure	X	X		

*The age requirement for law enforcement positions is 21.

FAMs and screener applicants must undergo a medical screening. TSA justifies medical evaluations of airport screeners as they "ensure that Federal screeners are able to provide the best security possible."[118] These medical requirements also help assure safety

116 "Understanding the Federal Hiring Process," Transportation Security Administration, accessed January 23, 2022, https://jobs.tsa.gov/federal-hiring-process.

117 Source: Transportation Security Administration.

118 Fabrice Czarnecki, *Medical & Psychological Guidelines for Transportation Security Officers* (Washington, DC: Transportation Security Administration, 2018), 1, https://jobs.tsa.gov/Resources/TSO_Medical_Guidelines.pdf.

in the workplace.[119] Nevertheless, the GAO has assessed that FAMs suffer from "extreme fatigue, mental health issues, difficulty maintaining a healthy diet, and increased frequency of illness due to duty hazards."[120]

In airports, all aviation employees, including TSA employees, airline employees, airport employees, and contractors, must obtain a secure identification display area (SIDA) badge to have unescorted access to sterile or restricted areas of the airport. To obtain a SIDA badge, an employee must be lightly vetted and credentialed by TSA. The vetting for SIDA badge access involves a fingerprint-based criminal records check to identify certain disqualifying criminal offenses, for example, aircraft piracy, murder, espionage, and armed robbery.[121] Such criminal offenses are only disqualifying if they occurred within 10 years of the employment application. The process also verifies one's lawful presence in the United States. Finally, a recurring check against the Terrorist Screening Center's watchlist and other databases rounds out the SIDA vetting.[122] A required SIDA screening and training process is renewed every year by each SIDA badge holder. Furthermore, aviation workers must self-report arrests or convictions to their leadership—a responsibility solely of the workers.[123] Otherwise, a foreign arrest or conviction might go undetected.

Because SIDA access is limited to aviation sector employees, TSA established the Transportation Worker Identification Credential (TWIC) designation for maritime employees. TSA is required to vet TWIC applicants by conducting a security threat

---

[119] Czarnecki.

[120] William Russell, *Aviation Security: Federal Air Marshal Service Has Taken Steps to Address Workforce Issues, but Additional Actions Needed* (Washington, DC: Government Accountability Office, 2020), 13, https://www.gao.gov/assets/gao-20-125.pdf.

[121] For a complete list of criminal offenses, see Fingerprint-Based Criminal History Records Checks, 49 C.F.R. 1542.209(e) (2009), https://www.govinfo.gov/app/details/CFR-2009-title49-vol9/CFR-2009-title49-vol9-sec1542-209.

[122] Transportation Security Administration, *SIDA Airport Security: Fiscal Year 2017 Report to Congress* (Springfield, VA: Transportation Security Administration, 2018).

[123] Fingerprint-Based Criminal History Records Checks, 49 C.F.R. 1542.209.

assessment, otherwise known as a background check.[124] A TWIC must be renewed every five years.

C. POLICIES AND PROCEDURES

TSA has implemented a policy to conduct agency-wide training to educate TSA employees and contractors on insider threats, policy compliance, and accountability.[125] In 2013, TSA implemented Management Directive 2800.17, *Insider Threat Program*, which provides TSA's policies, procedures, and implementation of the program.[126] As detailed in the directive,

> Pursuant to [Executive Order] 13587, TSA shall develop and implement an Insider Threat Program aimed at deterring, detecting, and mitigating insider threats to TSA's personnel, operations, information, and critical infrastructure consistent with the appropriate protections of privacy, civil rights, and civil liberties. The Insider Threat Program consists of Training and Awareness, Operations-Referrals and Mitigation, and Insider Threat Assessments.[127]

TSA established the Insider Threat Executive Steering Committee in October 2018 to promote consistent executive-level engagement. TSA's ITP is dispersed, so a more cohesive approach and oversight could yield benefits. As of February 2020, the GAO had recognized that TSA's *Insider Risk Roadmap* was under development. Once published, the roadmap would guide TSA's approach for insider risk mitigation moving forward. A completion date for the roadmap was unknown at the time.[128]

---

124 "TWIC," Transportation Security Administration," accessed August 22, 2021, https://www.tsa.gov/for-industry/twic.

125 Department of Homeland Security, Office of Inspector General, *Transportation Security Administration Has Taken Steps to Address the Insider Threat*.

126 Transportation Security Administration, *Insider Threat Program*, TSA Management Directive No. 2800.17 (Springfield, VA: Transportation Security Administration, 2013), https://www.tsa.gov/sites/default/files/foia-readingroom/insider_threat_program_2800.17pdf.pdf. This TSA management directive is available for public consumption via the Freedom of Information Act, but newer versions are not available to the public.

127 Transportation Security Administration, 5.

128 McNeil, *TSA Could Strengthen Its Insider Threat Program*, 36.

Though nearly a decade old, the ITP has failed to detect and prevent threats entirely. Although TSA requires limited background checks and conducts random employee screenings, it lacks a strategic plan to guide its ITP.[129] One of the primary deficiencies and reasons for failure is that the program does not effectively nor substantially reach the private sector organizations that interacts with TSA and the transportation sectors. On February 6, 2018, TSA Administrator David Pekoske explained to Congress that "TSA is responsible for securing nearly 440 federalized airports that facilitate upwards of 20,000 domestic flights per day and more than 2,000 outbound international flights per day."[130] Of those federalized airports, each comprises contractors; private airport and airline service workers; private airport employees; federal, state, and local law enforcement officers; and other government employees, all of whom may have regular access to secure spaces.[131] TSA engages in minimal screening and vetting of industry employees and has little oversight or input on industry employees or contractors working on TSA projects.

Currently, TSA utilizes a risk-based security approach that does not address all transportation sectors under its purview. As described by Jonathon Saucier, a cyber security consultant, "The Risk-Based approach is a systematic method that identifies, evaluates, and prioritizes threats facing the organization."[132] TSA's Management Directive 100.8 describes its risk-based approach, or *enterprise risk management*, as a "comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives."[133]

A popular publicly facing outcome of the risk-based security approach is TSA Pre-Check and its additional policies. Before TSA adopted a risk-based approach, all

---

[129] McNeil.

[130] Transportation Security Administration, *SIDA Airport Security*, 2.

[131] Transportation Security Administration, 2.

[132] "Why Take a Risk-Based (Instead of Compliance) Approach to Cybersecurity," CyLumena, accessed August 22, 2021, https://www.cylumena.com/insights/risk-based-cybersecurity/.

[133] Transportation Security Administration, *Enterprise Risk Management*, TSA Management Directive No. 100.8 (Springfield, VA: Transportation Security Administration, 2014), 1, https://www.tsa.gov/sites/default/files/foia-readingroom/enterprise_risk_management_100._8.pdf.

passengers were required to undergo standard screening. Currently, TSA Pre-Check members, people over the age of 75, military members, and children 12 or under benefit from expedited screening, while unknown and high-risk travelers are subject to the standard, more thorough screening.[134] Risk-based security benefits both travelers and the agency, enabling the agency to direct its resources, personnel, and funds to higher risks, including insider threats. In its *Insider Threat Roadmap*, TSA describes its path forward: implementing dynamic plans with an array of priorities enacted in phases to remain agile in response to new insider threats to the organization. For example, Priority 1 includes focusing on strategies (e.g., utilizing risk-scoring software and behavioral and situational metrics) to identify patterns over time.[135]

D. TECHNOLOGIES

TSA employs various cutting-edge technologies to detect threats to transportation among travelers. However, TSA utilizes only some of these technologies to screen TSA aviation employees at airports. The One Access Control system used for airport security can also be used to deter or prevent insiders from obtaining or providing unauthorized physical access to secure areas. The technologies that TSA uses for access control, such as lock and key, proximity badges, proximity badges with a required personal identification number (PIN), and fingerprint scanners, can be used in successive layers. Additionally, sensor towers attached to doors that lead to secure areas can detect any person who "piggybacks" or passes through the door with another person without providing proper credentials or a PIN. When the sensor tower is alerted, nearby cameras automatically pan toward the door to surveil and record the violation, allowing TSA to respond appropriately.[136]

TSA's IT sector conducts insider threat vulnerability assessments by continuously monitoring TSA's network for any behaviors indicative of insider threats, such as sending

134 "Risk-Based Security," Transportation Security Administration, accessed August 29, 2022, https://www.tsa.gov/news/press/factsheets/risk-based-security.

135 Transportation Security Administration, *Insider Threat Roadmap 2020*.

136 Grover, *Aviation Security*.

an email containing a violent threat or someone researching bombmaking while on TSA's network.[137] TSA monitors and collects data daily on all technology assets to determine any insider threat behaviors. For example, from firewall logs, it can monitor a change to bypass any website deemed inappropriate for government computers and any technology user who disables antivirus software. Finally, TSA conducts a daily review of the intrusion detection system log to monitor potential insider threat activities.[138] These passive monitoring technologies are not labor intensive, but they are invaluable defensive measures.

In 2018, TSA adopted another technology called the Advanced Threat Local Allocation Strategy (ATLAS) program, which automates and randomizes the location and schedule to screen airport employees entering secure areas of the airport. The ATLAS program determines where, when, and how airport employees get screened, and it can be tailored to local threat intelligence. This program could beat a ring of insider threats working together to bypass security screening or a lone wolf insider who can defeat or bypass standard screening.[139]

TSA invests in emerging technologies to increase security against evolving threats. Such emerging technologies include automated screening lanes, which utilize advanced technologies that increase security. TSA is also researching the impact of using biometric technology for identification, which can help defeat the use of fake or false identification attempts. Finally, the credential authentication technology ensures a person's identity, reservation, and pre-screening status are known almost instantly at the TSA security checkpoint.[140] Investments in emerging technologies, including artificial intelligence, probabilistic analytics, and data mining, enhance security and should be leveraged to screen airport staff and TSA employees, as outlined in TSA's *Insider Threat Roadmap 2020*.

---

[137] Department of Homeland Security, Office of Inspector General, *Transportation Security Administration Has Taken Steps to Address the Insider Threat*.

[138] Department of Homeland Security, Office of Inspector General.

[139] McNeil, *TSA Could Strengthen Its Insider Threat Program*.

[140] "Emerging Technology," Transportation Security Administration, accessed August 29, 2022, https://www.tsa.gov/travel/security-screening/emerging-technology.

E. KEY FINDINGS

TSA employs a layered approach to screening incoming employees; however, the depth and breadth of the screening may not be appropriate for all types of employees. For example, TSA does not polygraph or require financial disclosure for the screening officers at airports. Notably, transportation security officers have full access to the airport and the ability to bypass security at any time. Additionally, continual vetting of employees, once they are hired, is minimal.

TSA has made investments in technologies to aid in autonomous monitoring, but the push for advanced technology is motivated by the need to reduce wait times and improve the traveler's experience. Thus, most investments have been in passenger security rather than in insider threats. Where technology for passive detection has been implemented, large swathes of the workforce are excluded from monitoring. For example, once the initial hiring screening is completed, screening officers who develop harmful intentions may go undetected because they rarely use TSA's intranet, which prevents the passive detection of threats. ATLAS has the potential to help mitigate this weakness but has not proven effective at detecting threats.

Last, even though TSA's purview includes air travel, rail, surface streets, pipelines, and maritime transportation, air travel is the primary modality of focus, perhaps to the point of neglect of other modalities. TSA recognizes that insider threats are a significant issue, yet more decisive actions are needed to mitigate and detect potential bad actors within TSA. This chapter has demonstrated that insider threat detection and mitigation are still lacking at TSA despite the implementation of several noteworthy policies, procedures, and technologies. The next chapter examines how three other national-level agencies have dealt with similar insider threat issues.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. COMPARATIVE ANALYSIS

This chapter presents a comparative analysis of the FBI, DOD, and CPNI, focusing on the agencies' strategies for addressing insider threats and comparing strengths and weaknesses of their insider threat reduction efforts. These organizations were chosen for several reasons. The FBI and DOD screen broad types of personnel and have been ravaged by insider threats. The UK's similar laws and insider threats to the United States make its CPNI a suitable agency for comparison. Analyzing these organizations might lend insight into TSA's prevention efforts.

A. FEDERAL BUREAU OF INVESTIGATION

The FBI is the United States' premier law enforcement organization, and its mission is to "protect the American people and uphold the Constitution of the United States."[141] More specifically, the FBI is tasked with protecting the United States from terrorism, foreign espionage, cyberattacks, criminal activity, public corruption, white-collar crimes, and violent crimes, and it could be entrusted with anything that poses a threat to the United States.[142] The FBI's structure comprises the following divisions: National Security, Criminal and Cyber Crimes, Intelligence, Science and Technology, Information Technology, and Human Resources. The bureau's offices extend across the United States and the world, with 56 field offices in the United States, primarily in major cities; an additional 350 satellite offices; and 60 international offices as legal attachés housed in U.S. embassies.[143]

The FBI has a workforce of over 35,000—half of whom are unsworn personnel—including sworn law enforcement officers, intelligence analysts, language specialists, scientists, and IT specialists.[144] The bureau is also responsible for contractors and other

141 "Mission & Priorities," Federal Bureau of Investigation, accessed October 7, 2021, https://www.fbi.gov/about/mission.

142 Federal Bureau of Investigation.

143 Federal Bureau of Investigation.

144 Federal Bureau of Investigation.

personnel, for example, local police officers or other federal employees assigned to an FBI task force, office, or program.[145]

1. Screening

The employee screening process for FBI applicants varies slightly between special agents and non–law enforcement staff. Special agents, who serve as criminal investigators, are typically assigned to strenuous or dangerous activities while dealing with criminals and the criminal world. The professional non–law enforcement staff support the agents in the field. All applicants undergo a background investigation, a thorough and rigorous process that reviews the last 10 years of the applicant's life and verifies biographical information. This process includes interviews with family members, friends, and current and former employers to obtain a frame of reference and understanding of who the applicant is as a person, friend, and employee.[146]

The FBI background investigation is a bifurcated process that evaluates a person's suitability for the job and vets any potential security risks to the FBI or the country. The suitability segment of the background investigation examines applicants' and employees' personal integrity, as previously detailed. The FBI also examines the applicant's personal conduct, education, and employment histories, verifying the applicant's affiliations and loyalty to the United States.[147] The FBI also investigates financial backgrounds for all employees and applicants by conducting credit checks. In addition, a pre-employment polygraph is administered for all potential employees with access to FBI information and spaces.[148] Last, personnel security specialists review all information from the individual's background investigation and polygraph to determine whether the applicant meets the

---

145 Jason Miller, "FBI Boosts IT Efforts to Protect Itself from Rogue Employees," Federal News Network, May 14, 2018, https://federalnewsnetwork.com/reporters-notebook-jason-miller/2018/05/fbi-boosts-it-efforts-to-protect-itself-from-rogue-employees/.

146 "Background Checks for New Applicants," April 17, 2009, in *Inside the FBI*, produced by the Federal Bureau of Investigation, podcast, MP3 audio, 6:48, https://www.fbi.gov/audio-repository/news-podcasts-inside-background-checks-for-new-applicants.mp3/view.

147 Federal Bureau of Investigation, "Background Checks for New Applicants"; Henry M. Holden, *To Be an FBI Special Agent* (St. Paul, MN: Zenith Press, 2005).

148 "Special Agent – Law Enforcement or Military Veteran Background," USA Jobs, accessed October 30, 2021, https://www.usajobs.gov:443/GetJob/ViewDetails/463469600.

standards to work with or for the FBI and to obtain a top-secret, sensitive compartmented information clearance.

2. Policies

Limited policies related to insider threats are immediately and readily available for general public consumption. In 2009, the FBI produced the *Personnel Security Clearance and Access Policy Guide* for all FBI and non-FBI personnel with access to IT or classified information. This document details how the FBI conducts its personnel security, outlining the following eligibility requirements for all applicants: Electronic Questionnaires for Investigations Processing (e-QIP) or Standard Form 86, fingerprints for processing, a credit report, access to financial records, an illegal drug history, health information, and a loyalty agreement. Applicants must also complete a background investigation that details the past 10 years, a personnel security interview, and a drug test. Finally, the FBI conducts a polygraph and physical examination depending on the job.[149] Notably, the vetting process is different for the FBI's non-employee personnel, such as taskforce officers, who may bypass some requirements because the individual has theoretically been vetted by one's agency.

In 2011, President Barack Obama signed Executive Order 13587, which requires executive branch organizations, including the FBI, to increase the protection of classified information on government networks. The goal of this executive order was to prevent the unauthorized release of classified information from insiders by addressing gaps in policy for information systems security.[150]

In 2014, the FBI created the Insider Threat Risk Board (ITRB), which meets every quarter. Representatives from Finance, Human Resources, and IT are invited to this meeting to inform the board of any factors that might be indicative of potential insider

[149] Federal Bureau of Investigation, *Personnel Security Clearance and Access Policy Guide* (Washington, DC: Federal Bureau of Investigation, 2009), https://vault.fbi.gov/personnel-security-clearance-and-access-policy-guide-0192pg/personnel-security-clearance-and-access-policy-guide-0192pg-part-01-of-01.

[150] Exec. Order No. 13587, 3 C.F.R. 276 (2011), https://www.govinfo.gov/content/pkg/CFR-2012-title3-vol1/pdf/CFR-2012-title3-vol1-eo13587.pdf.

threats. The ITRB establishes mitigation plans for FBI employees or associates who pose a potential internal threat to the organization. This board makes a final determination if FBI divisions or offices cannot agree on a plan of action or mitigation for a potential insider threat.[151] Every two years, FBI staff work together with the ITRB to prevent single anomalies from proliferating into significant insider threats while reducing entry barriers for employee participation.[152]

3. Procedures

Although background investigations are a main staple of the screening process, there have been failures to detect suitability and security risks. In response to one such failure, the acting deputy assistant director of Security Programs and Countermeasures for the FBI testified before the Senate Judiciary Committee in July 2001 about the FBI's screening program and proposed changes to further enhance the security process.[153] A task force of FBI assistant directors found that background investigations should be conducted by a separate internal security unit well versed in counterintelligence issues to avoid security risks. This unit is now staffed with agents, civilians, and contractors.[154]

The key findings of an FBI Office of Inspector General investigation in 2003 helped to establish current FBI background investigations processes.[155] The previous system had discouraged a thorough review due to the investigators' lack of access to employees' basic information, such as their employee files, credit reports, and security records, which tracked any security violations. Additionally, the background investigators had not been interviewing the employees under investigation. The Office of Inspector General had found

[151] Department of Justice, Office of the Inspector General, *Public Summary*; Miller, "FBI Boosts IT Efforts."

[152] Miller, "FBI Boosts IT Efforts," 1.

[153] Kenneth H. Senser, "Testimony before the Senate Judiciary Committee," Federal Bureau of Investigation, July 18, 2001, https://www.fbi.gov/news/testimony/review-of-the-fbi-security-program-and-its-transformation.

[154] Senser.

[155] Department of Justice, Office of the Inspector General, "Investigating the Espionage Activities of Robert Philip Hanssen."

that FBI background investigations were a mere collection of information about employees that lacked analysis and failed to make investigative recommendations.[156]

As mentioned previously, the FBI utilizes polygraph examinations for applicants and current employees periodically. The scope of the polygraphs may include national security, a suitability issue, or counterintelligence questions. Employees with special access to sensitive investigations or programs are polygraphed more frequently than those without access. A polygraph may also be used for employee misconduct or other internal inquiries that warrant internal investigations.[157] Moreover, FBI employees who leave for or return from permanent foreign assignments undergo polygraphs.[158]

FBI special agents and other employees with special and sensitive access are required to complete an annual financial disclosure form—a means of gathering and analyzing employee information regularly.[159] The FBI's financial disclosure team adopts a "red team" approach in its analysis whereby analysts emulate potential actions of insider threats attempting to hide assets or business dealings. This process could help detect vulnerabilities not readily apparent.[160]

In addition, the FBI delivers security debriefings and exit interviews for personnel who no longer work for the bureau or need their clearance.[161] Exit interviews might identify counterintelligence concerns and employee or management issues. Andrée Rose of PERSEREC claims, "The purpose of the Federal Government's personnel security program is to determine if applicants for access to classified information are loyal,

156 Department of Justice, Office of the Inspector General.

157 Senser, "Testimony before the Senate Judiciary Committee."

158 Senser.

159 Department of Justice, Office of the Inspector General, "Investigating the Espionage Activities of Robert Philip Hanssen."

160 Miller, "FBI Boosts IT Efforts."

161 Federal Bureau of Investigation, *Personnel Security Clearance and Access Policy Guide*.

trustworthy, and reliable."[162] This definition extends to obtaining pertinent information over an individuals' entire tenure with the organization.

4. Technologies

The FBI utilizes multiple technologies to strengthen its resolve against insider threats. Analysts cannot sort through every detail of the vast data collected from approximately 70,000 staff members and contractors. Accordingly, the FBI uses various data management tools to help track potential indicators made manifest during investigations, polygraphs, and regular duty. First, the FBI uses the Insider Threat Analysis Platform (InTAP) to analyze models, triggers, and data sets to identify potential insider threats.[163] InTAP is designed explicitly for the large volumes of data obtained from the FBI's employees and contractors.[164] Using data points, the platform determines whether an investigator should probe potential issues further. Second, the FBI created Javelin, a tool to monitor all internal referrals that involve derogatory information about an employee, such as a security violation, internal espionage, or misconduct. Javelin also keeps records of polygraph examination results, past associates, and other investigative information, and analysts can query information about specific employees via a simple name search.[165]

These programs also work best when all the information obtained is accessible through a database. One means of information storage is the FBI's Automated Case Support (ACS) system, a repository for all case-related information built as a secure virtual case file. However, some agents have expressed concern over the system's level of data

---

[162] Andrée E. Rose et al., *Leveraging FBI Resources to Enhance Military Accessions Screening and Personnel Security Vetting*, OPA Report No. 2020–080-O (Seaside, CA: Defense Personnel and Security Research Center, 2020), 37.

[163] Miller, "FBI Boosts IT Efforts," 1.

[164] Monica Jackson, "FBI Employs AI, Big Data Analytics Systems to Identify Insider Threats," ExecutiveGov, August 24, 2018, https://www.executivegov.com/2018/08/fbi-employs-ai-big-data-analytics-systems-to-identify-insider-threats/.

[165] Miller, "FBI Boosts IT Efforts"; Jackson, "FBI Employs AI, Big Data Analytics Systems."

protection and avoid recording sensitive case information in ACS.[166] However, for Javelin and InTAP to be optimally functional, all information must be entered into ACS.

These tools are not entirely sufficient on their own, as the FBI acknowledges that insider threats are not wholly information technology–based. Because human factors can escape programs such as Javelin and InTAP, behavioral monitoring techniques need to be developed and utilized for an all-encompassing approach. Statistical modeling and technical monitoring to predict malicious behavior have not been entirely successful. At this time, technical monitoring cannot predict or perceive human motives or behavior.[167]

5. Critical Incident 1: Robert Hanssen

One of the most notorious and damaging spies in U.S. history was former FBI Special Agent Robert Hanssen, who engaged in multiple periods of active espionage with Russian against the United States. Over his 25-year career with the FBI, almost half of his time was spent spying for the Russian government.[168] In the mid-1980s, the Central Intelligence Agency (CIA) and FBI lost many human intelligence assets in the Soviet Union to murder or arrest. Hanssen successfully provided extremely sensitive and highly classified materials to Russian agents.[169] In 2001, FBI agents arrested Hanssen and charged him with committing espionage against the United States on behalf of the former Soviet Union and Russia. Hanssen pled guilty to 15 counts of espionage and is serving a lifetime prison sentence without the possibility of parole.[170]

Hanssen leveraged the lack of security features in ACS, easily gaining unimpeded access to sensitive information about technical operations and acquiring more information on FBI methods for conducting intelligence operations and ongoing investigations.

166 Harry Goldstein, "Who Killed the Virtual Case File?," *IEEE Spectrum*, September 1, 2005, https://spectrum.ieee.org/who-killed-the-virtual-case-file.

167 I. Hilmi Elifoglu, Ivan Abel, and Özlem Taşseven, "Minimizing Insider Threat Risk with Behavioral Monitoring," *Review of Business: Interdisciplinary Journal on Risk and Society* 38, no. 2 (2018): 66, https://www.stjohns.edu/sites/default/files/uploads/review-of-business-382-june_2018.pdf.

168 Department of Justice, Office of the Inspector General, "Investigating the Espionage Activities of Robert Philip Hanssen."

169 Department of Justice, Office of the Inspector General.

170 Department of Justice, Office of the Inspector General.

Hanssen not only exploited the FBI's database system to provide information to his Russian handlers but also used it to verify whether he was under investigation for espionage.[171] Hanssen informed investigators that he had ample opportunity to spy on the United States for Russia.

Investigators and psychologists opine that many factors contributed to Hanssen's espionage. First, Hanssen suffered from low self-esteem and an extreme need to appear intellectually superior. He also lacked morals and felt that he was above the law. Additionally, he had an enduring obsession with espionage, which furthered his proclivity to actual espionage, and he received financial incentives from his Russian handlers. Last, the lack of hurdles and low chance of being caught and convicted further incentivized Hanssen to betray the FBI and the United States.[172] Furthermore, while background investigations are a regular part of intelligence and law enforcement organizations and can be effective, Hanssen received only one background investigation during his two-decade career. Even with that background investigation, derogatory information had been obtained but never resolved.[173]

During Hanssen's career, the FBI lacked proper policies to deter or detect insider threats. The initial FBI employee screening did not indicate future intent, so new screening and monitoring methods have since been created. With Hanssen's activities, the FBI also realized that its current programs and policies were neither effective nor robust enough. Last, existing technologies neither deterred nor detected Hanssen's illegal activities at the time they occurred. However, in the aftermath, the FBI expanded its polygraph program after a review from a security task force. While the IC has criticized the use of polygraphs for potential false positives—whereby innocent people are found to be deceptive during their polygraph examinations—the FBI maintains that the adverse effects of occasional

171 Goldstein, "Who Killed the Virtual Case File?"

172 Department of Justice, Office of the Inspector General, "Investigating the Espionage Activities of Robert Philip Hanssen."

173 Department of Justice, Office of the Inspector General.

false positives do not outweigh the damage that an insider can cause to the FBI and the United States.[174]

6. Critical Incident 2: Shamai Leibowitz

The FBI employed Shamai Leibowitz, a dual Israeli and U.S. citizen, as a linguist. Between January and August 2009, Leibowitz leaked five sensitive documents comprising approximately 200 pages of classified information about U.S. IC activities to an unknown blogger.[175] Leibowitz was motivated to disseminate this classified information due to his perception of the U.S. government's wrongdoings. From Leibowitz's perspective, there had been a significant abuse of power in the government.[176] The FBI and other federal government agencies have a clear policy for whistleblowers. Through federal policy, the FBI could have classified Leibowitz as a whistleblower—an employee who exposes organizational information deemed illegal, fraudulent, or wasteful—had he utilized the proper channels to voice his perception of government-sanctioned illegal behavior. Instead, he was charged under the Espionage Act, 18 U.S.C. § 798(a), with one count of disclosure of classified information.[177] Violating the law and the procedure for reporting led to his conviction.

7. Key Findings

The FBI had suffered from severe deficiencies in all aspects of its internal security programs—from personnel, to computer and document security, to security training and compliance. In a review of the FBI's performance in the Hanssen case, Glen Fine with the Office of Inspector General determined, "These deficiencies led to the absence of effective deterrence to espionage at the FBI and undermined the FBI's ability to detect an FBI

174 Senser, "Testimony before the Senate Judiciary Committee."

175 "Shamai Leibowitz Case Study: Unauthorized Disclosure," Center for Development of Security Excellence, accessed September 27, 2021, https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-shamai-leibowitz.pdf.

176 Center for Development of Security Excellence.

177 "Former FBI Contract Linguist Pleads Guilty to Leaking Classified Information to Blogger," Department of Justice, December 17, 2009, https://www.justice.gov/opa/pr/former-fbi-contract-linguist-pleads-guilty-leaking-classified-information-blogger.

mole."[178] The FBI's applicant and internal screening processes were either extremely lax, nonexistent, or disconnected from other screening methods.[179]

The security program initiated a self-assessment in 2000 because of Hanssen's significant security breach. Kenneth H. Senser, acting deputy assistant director of Security Programs and Countermeasures for the FBI, testified before the U.S. Senate that "the program was fragmented and dispersed across several different divisions. It lacked an integrated vision, and security initiatives were often poorly coordinated, inefficient, and not as effective as possible."[180] While the FBI created several new and significantly improved internal monitoring systems, programs, and positions to combat insider threats, this overhaul of insider threat mitigation has not been perfect.

There have also been issues with the FBI's internal security systems, which require buy-in from all employees for them to work properly. Even with improvements to the bureau's security culture and protocols, no system can prevent or detect every insider threat. However, the speed and accuracy of detection can make a significant difference in preventing and reducing damage.[181]

Furthermore, the FBI's current system is significantly fragmented. First, various internal departments within the FBI obtain data related to insider threats, but most of them fail to communicate with other offices. Second, although multiple divisions may notice potential indicators of an insider threat, each has access to only one piece of the puzzle, and a lack of integrated oversight can negate all updates to an internal security program. Third, the security executive should serve as a stand-alone entity that answers only to the director of the FBI. Fourth, some have recommended that the internal security program be detached from the FBI's National Security Division, so it does not overburden investigators

178 Department of Justice, Office of the Inspector General, "Investigating the Espionage Activities of Robert Philip Hanssen," 2.

179 Senser, "Testimony before the Senate Judiciary Committee."

180 Senser.

181 Senser.

or create additional barriers to information access, and that a centralized reporting system be established for security violations.[182]

B. DEPARTMENT OF DEFENSE

The DOD is America's most well-known government organization and one of the oldest departments. Its mission is to deter war and protect the nation.[183] The DOD's 4,800 locations span the United States and the world, with overseas sites in 160 countries. With a budget of $740.5 billion, the DOD comprises 2.91 million employees, including active-duty military and civilians, as well as defense contractors, detailed assignments, and local nationals with access to DOD spaces and information.[184] This vast span of locations and personnel stresses the importance of an all-encompassing internal security program.

The DOD consists of the Army, Marine Corps, Navy, Air Force, and Space Force as well as the National Security Agency (NSA), Defense Intelligence Agency (DIA), National Geospatial-Intelligence Agency, and National Reconnaissance Office.[185] Internal security varies among these different agencies under one large organization. The DOD has 11 joint combatant commands, composed of two or more military branches. Each combatant command is tasked with a geographic or functional mission. For example, the United States Northern Command, along with DOD partners, works with and houses Canadian and Mexican military components, all of whom have access to DOD information and spaces.[186] This North American partnership leads to concerns regarding internal screening policies and reciprocity with other U.S. and international organizations.

---

[182] Senser.

[183] "About," Department of Defense, accessed October 13, 2021, https://www.defense.gov/About/.

[184] Department of Defense.

[185] "Members of the IC," Office of the Director of National Intelligence, accessed November 22, 2021, https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

[186] "About," U.S. Northern Command, accessed November 22, 2021, https://www.northcom.mil/About-USNORTHCOM/.

1. Screening

The screening process for the DOD varies depending on the type of applicant, position, location, and duty. All candidates for active military duty must meet demanding moral and character standards for the armed forces, involving questions about criminal misconduct, deviant behavior, and substance abuse. Active-duty applicants may be precluded from military service if they display a current or previous pattern of these behaviors.[187] One might argue that moral character does not correlate with military performance, but it may predict attitudes toward rules and structure. Utilizing moral standards may reduce attrition in the armed services and uphold the morale and image of each branch.[188] Again, moral standards vary from one service to another.

Military recruiters evaluate, test, and screen each applicant. Recruiters evaluate the applicants' background, determine which military duties best complement the recruits' educational and job history, and complete the application process by obtaining vital documents.[189] Part of the screening process involves a thorough interview covering the applicants' educational and employment background and a psychological evaluation. Recruiters can stop the application process if they determine potential applicants are unfit for recruitment and unable to obtain a waiver.

The DOD requires that all active-duty members maintain a minimum physical fitness standard under the philosophy that they are warriors irrespective of their assigned job duty.[190] DOD Instruction 1308.3 states, "It is DOD policy that physical fitness is essential to combat readiness and is an important part of the general health and well-being

[187] Barbara Means, *Moral Standards for Military Enlistment: Screening Procedures and Impact* (Alexandria, VA: Human Resources Research Organization,1983), https://apps.dtic.mil/sti/citations/ADA135995.

[188] Means.

[189] Shailynn Krow, "Military Recruiter Job Responsibilities," *Houston Chronicle*, accessed November 22, 2021, https://work.chron.com/military-recruiter-job-responsibilities-12701.html.

[190] Paul R. Sackett and Anne S. Mavor, eds., *Assessing Fitness for Military Enlistment: Physical, Medical, and Mental Health Standards* (Washington, DC: National Academies Press, 2006), https://doi.org/10.17226/11511.

for Armed Forces personnel."[191] The armed forces' multifaceted approach to screening includes general fitness for enlistment and physical requirements, which vary slightly for each branch.

Each military applicant must meet a mental health standard in conjunction with physical screenings. The mental health evaluation includes a psychiatric evaluation, which evaluates personality, emotional stability, and psychiatric diseases. The DOD's *Medical Standards for Appointment, Enlistment, or Induction in the Armed Forces* outlines specific guidelines for disqualifying mental health conditions. These disqualifying parameters range from prior psychiatric hospitalization for any cause to depressive disorders if certain conditions are met.[192]

The DOD utilizes electronic financial credit checks and searches for criminal records to gauge hiring suitability. Disqualifying criminal activity includes substance abuse and sexual misconduct. Some of these criminal activities may be overlooked with a waiver.[193]

Finally, the services conduct a tattoo screening during the medical exam to gauge the applicants' affiliations with gangs or domestic extremist groups. This screening also considers the meaning of the tattoos to the applicant and any information about such tattoos found through an online search engine. The tattoos alone could mean little, but combined with other tattoos on the body, they could mean something else entirely. Photographs of cryptic tattoos are sent to the Cryptology and Racketeering Records Unit, whose specialists examine such communications, records, and symbols.[194]

Most civilian employees in the DOD undergo less rigorous pre-employment screening than active-duty members. Civilian employee applicants undergo interviews,

---

[191] Department of Defense, *DOD Physical Fitness and Body Fat Programs Procedures*, DOD Instruction 1308.3 (Washington, DC: Department of Defense, 2002), 2, https://biotech.law.lsu.edu/blaw/dodd/corres/html/13083.htm.

[192] Department of Defense, *Medical Standards for Military Service: Appointment, Enlistment, or Induction*, DOD Instruction 6130.03, vol. 1 (Washington, DC: Department of Defense, 2021).

[193] Sackett and Mavor, *Assessing Fitness for Military Enlistment*.

[194] Rose et al., *Leveraging FBI Resources*.

background investigations, credit checks, drug tests, and verification of U.S. citizenship.[195] Once applicants have a formal job offer, they undergo a security interview with their background investigator, the scope of which is determined by the sponsoring agency. That interview verifies their identity and clarifies background information. Then, a background investigator verifies previous employment and education and interviews personal and work associates, landlords, family members, and neighbors to vet the applicants.[196] Finally, the sponsoring agency requires that employees undergo and obtain favorable results on a credit check and urinalysis to be officially offered employment.

For the DOD's intelligence components, such as the NSA and DIA, entry barriers for employment are rigorous due to the extremely sensitive nature of performing intelligence work and dealing with classified information. The screening methods are effectively standard for all personnel with access to sensitive information or spaces, including military members, civilians, contractors, and detailees. The DOD's credibility assessment—typically involving a polygraph—is a multi-disciplinary field procedure that gauges the truthfulness of applicants and employees.[197] The NSA and DIA require all personnel to pass a polygraph test with personal suitability or counterintelligence scope to access their spaces and information.

2. Policies

The DOD has numerous policies to address insider threats, including responses to overall threats and specific incidents. The National Defense Authorization Act for Fiscal Year 2012 required the DOD to create a system to protect information-sharing and mitigate insider threats for all DOD systems.[198] The resulting program includes centralized monitoring and detection of unauthorized activities related to IT, including all information

195 "Application Process," U.S. Intelligence Community Careers, accessed October 14, 2021, https://www.intelligencecareers.gov/application-process.

196 "Investigations, Adjudications and Clearance Processes at a Glance," Defense Counterintelligence and Security Agency, accessed November 25, 2021, https://www.dcsa.mil/mc/pv/mbi/gicp/.

197 Aftergood, "DOD Adds 'Credibility Assessment' to Polygraph Program."

198 National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112–81, 125 Stat. 1298 (2011), https://www.govinfo.gov/content/pkg/PLAW-112publ81/pdf/PLAW-112publ81.pdf.

ports, removable media ports, and unusual authorized user activities, such as searches or information crossover from data systems. The act also requires DOD organizations to integrate, update, and expedite the security clearance process for determining the suitability of applicants, reviewing personnel, and classifying materials.[199] These requirements aim to streamline, standardize, and increase communication between DOD organizations.

In 2014, DOD Directive 5205.16 created the DOD's ITP. This program requires all DOD entities to integrate and synchronize their programs. As detailed in the directive, each department should disseminate information to other organizations to prevent insiders from evading detection:

> The DOD Insider Threat Program will gather, integrate, review, assess, and respond to information derived from [counterintelligence], security, cybersecurity, civilian and military personnel management, workplace violence, [anti-terrorism] risk management, [law enforcement], the monitoring of user activity on DOD information networks, and other sources as necessary and appropriate to identify, mitigate, and counter insider threats.[200]

Due to a significant data breach of the Office of Personnel Management (OPM) in 2015, foreign hackers obtained highly sensitive security clearance data of all background investigations, including personal and biographical information on millions of government employees and applicants.[201] In 2019, Executive Order 13869 transferred the responsibility of federal background investigations from the OPM to the DOD's Defense Counterintelligence and Security Agency (DCSA).[202] One of the benefits of this transfer is that the DOD may now vet information on any insider threat indicators.

---

199 National Defense Authorization Act for Fiscal Year 2012.

200 Department of Defense, *The DOD Insider Threat Program*, DOD Directive 5205.16 (Washington, DC: Department of Defense, 2017), 2, https://irp.fas.org/doddir/dod/d5205_16.pdf.

201 Gregory C. Wilshusen and Nabajyoti Barkakati, *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*, GAO-17-614 (Washington, DC: Government Accountability Office, 2017), https://www.gao.gov/assets/gao-17-614.pdf.

202 Exec. Order No. 13869, 84 Fed. Reg. 18125 (April 24, 2019), https://www.federalregister.gov/documents/2019/04/29/2019-08797/transferring-responsibility-for-background-investigations-to-the-department-of-defense.

3. Procedures

The DOD has numerous programs to address insider threats. One of the most recent and encompassing programs has been the DOD's Insider Threat Management and Analysis Center (DITMAC), established in response to the 2013 Washington Navy Yard shooting and other malicious attacks by DOD insiders. DITMAC is an information-sharing hub for all 43 DOD organizations and serves as a collaborative insider defense resource.[203] When any DOD entity has an insider threat concern, the organization can provide its information to DITMAC, whose designated experts analyze the information. DITMAC provides recommendations to the presenting organization and cross-references the insider threat's information with any other reports or incidents within the DOD. DITMAC is a vital organization that can prevent DOD insiders from causing more damage.

The DCSA is devoted to safeguarding the United States' physical and virtual trusted workforce and workspaces. It includes personnel vetting and critical technology protection, supported by counterintelligence and training, education, and certification functions. Each year, the DCSA provides services for over 100 federal entities, oversees 10,000 cleared companies, and conducts approximately two million background investigations. The DCSA may be best suited for recommending and prescribing best practices for cleared industry members and other DOD organizations.[204]

Another program adopted by the DOD is a month-long awareness campaign every year to educate and request the help of all DOD personnel in reporting any suspicious activity witnessed in the line of duty. In addition to educating personnel, this campaign advocates awareness, including cultural awareness. It is not uncommon for DOD employees to feel uneasy about alerting security to a coworker's actions or even self-

[203] Center for Development of Security Excellence, *DOD Insider Threat Management Analysis Center (DITMAC) Short Student Guide* (Linthicum Heights, MD: Center for Development of Security Excellence, 2016), https://www.cdse.edu/Portals/124/Documents/student-guides/shorts/INT100-guide.pdf.

[204] "About Us," Defense Counterintelligence and Security Agency, accessed August 14, 2022, https://www.dcsa.mil/About/.

reporting infractions. Nevertheless, personal indicators of potential insider threat behavior do not automatically mean an employee is an insider threat.[205]

4. Technologies

The DOD is working to upgrade the Zero Trust Architecture (ZTA) for portions of the community. ZTA provides more robust and encompassing network security than the previous platform does, adopting a security stance for DOD users with carte blanche access to networks by blocking or tracking them.[206] It can prevent insider threats from compromising large quantities of classified and sensitive information and reduce information access to users by allowing access only to employees and organizations that need to know specific information.[207] Significant harm can be caused by compromised information, so moderating general access while providing the proper parties access to information is vital.

5. Critical Incident 1: Washington Navy Yard Shooting

On September 16, 2013, DOD contractor Aaron Alexis arrived at the Navy Yard in southeast Washington, DC, home to the U.S. Naval Sea Systems Command on the banks of the Anacostia River. As a Navy contract employee with a secret-level clearance, Alexis had full access to the building and a solid understanding of the location and employees within it. With a concealed modified shotgun, Alexis entered the building and killed 12 people and injured three others. Approximately one hour after he started the shooting rampage, police killed Alexis in an exchange of gunfire. There is reason to believe Alexis suffered from mental health issues, and he had a pattern of employee misconduct.[208] The

---

[205] Lopez, "DOD Program Aims to Deter Insiders from Harmful Acts."

[206] Department of Defense, *Zero Trust Reference Architecture* (Washington, DC: Department of Defense, 2022), https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

[207] Department of Defense, *Zero Trust Reference Architecture*; Kurt DelBene, Milo Medin, and Richard Murray, *The Road to Zero Trust (Security)* (Washington, DC: Defense Innovation Board, 2019), https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_%28SECURITY%29_07.08.2019.PDF.

[208] Department of Defense, *Internal Review of the Washington Navy Yard Shooting* (Washington, DC: Department of Defense, 2013), https://permanent.fdlp.gov/gpo46879/DOD-Internal-Review-of-the-WNY-Shooting-20-Nov-2013.pdf.

attack by Alexis marks the second deadliest mass murder by shooting on a U.S. military base.

DOD policy has not changed much since the 2013 incident. Alexis had a valid secret clearance and was subject to the same pre-employment standards as all Navy contractors with that clearance. In 2004, local police arrested Alexis for an event that involved a firearm. When Alexis was filling out his clearance paperwork, he declared he had not been charged with a felony or arrested within the last seven years because the charges from 2004 had been dismissed.[209]

A failure to follow procedures prevented naval authorities from intervening or restricting access to Navy assets, thus facilitating Alexis's attack. An internal DOD review found that the OPM, the organization charged with conducting background investigations, had failed to obtain critical information about Alexis. Multiple sections in Alexis's background investigation were incomplete. The OPM neglected to resolve discrepancies because it had either overlooked them or failed to clarify inconsistencies.[210]

The Department of the Navy provided Alexis with a secret security clearance with specified conditions. However, there was no oversight to ensure he adhered to the requirements for maintaining his clearance. Alexis suffered from financial issues but was still issued a clearance with the caveat and a warning letter stating he must attend financial counseling and pay off outstanding debt. There was no follow-up mechanism to verify whether he complied with these requirements.[211]

The Experts, Inc., the contract company that employed Alexis at the time, did not have access to information about his previous personal conduct and provided him with a clearance to fulfill his duties. To gain access to the Navy Yard, Alexis needed only a military ID and a base pass, which were afforded him for his contracting duties. Cleared employees need not be screened when entering the Navy Yard and most buildings. Even

[209] Department of Defense.

[210] Department of Defense.

[211] Department of Defense.

today, the weapon that Alexis brought onto base and in the building would not have been detected. The current policies in place would have done little to prevent this attack.

The Experts, Inc., failed to follow procedures and report Alexis's concerning behaviors and actions. In August 2013, Alexis exhibited erratic behavior, which might have indicated psychological instability. The employer failed to report these actions or request guidance from the Navy on how to proceed. If the company had followed policy, Alexis might have had his clearance and access temporarily suspended before the attack. When asked why it had failed to follow policy, Alexis's employer cited concerns about jeopardizing his career or clearance by reporting the erratic behavior. This failure to follow policy provided Alexis many opportunities to avoid detection.

During the attack, the Navy Yard had a competent closed-circuit video camera system staged around the building that detected Alexis's movements during and after the rampage. Besides this technology, no others were used to prevent this incident.

6. Critical Incident 2: Edward Snowden

NSA contractor Edward Snowden leaked thousands of classified NSA documents to journalists in 2013. The 1.5 million stolen classified documents captured international attention when multiple media outlets published some of the stolen information. This classified information leak caused grave damage to U.S. intelligence programs and national security; however, the full extent of damage is still unknown. While working with U.S. intelligence, Snowden began questioning and objecting to the programs impacting personal privacy interests. Snowden claimed he had attempted to raise these ethical concerns via the proper channels to no avail. He used low-tech methods to steal information from the NSA's network, including accessing standard network administrator tools to download 1.5 million documents and exploiting loopholes to avoid NSA's network security detection.[212]

Due to the Snowden leaks, the ODNI complies with the President's National Insider Threat Policy for all top-secret networks within the IC. Nevertheless, this compliance

[212] House of Representatives, *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden* (Washington, DC: House of Representatives, 2016), https://www.congress.gov/114/crpt/hrpt891/CRPT-114hrpt891.pdf.

started only after Snowden significantly damaged national security and bypassed the NSA's security protocols.[213] The NSA advertises these requirements to its cleared contractors.

Snowden revealed a pattern of lying, exaggerating the facts, and fabricating information on his résumé, which was not adequately detected until after he had leaked secure documents. He had also expressed concern about employee morale while a contractor for the CIA. These incidents were not adequately documented or articulated in his personnel file. Therefore, his CIA clearance lacked critical information when he applied for NSA contractor jobs. In June 2012, Snowden was reprimanded for going outside his chain of command regarding concerns over how computer updates should be managed.[214] Shortly after that incident, Snowden started to aggregate classified information. The CIA's and NSA's failure to follow procedures and properly document Snowden's questionable behavior allowed him to continue accessing classified information.

The NSA had numerous technologies and security measures in place to prevent an illegal download of classified information from the NSA network, such as access logs and audits if anyone tried to remove data from the network. Snowden utilized his network systems administrator authority to infiltrate sections of the network that he could not typically access. Snowden also requested the assistance of a coworker to gain access to information that was not privy to him.[215] Finally, he took advantage of loopholes to gain access to and remove information from the NSA's network.

7. Key Findings

The DOD is traditionally considered a secure and risk-averse organization. Despite having a robust security presence, the Office of the Inspector General found the following deficiencies in the NSA's security policy:

---

213 "Commercial Solutions for Classified (CSfC) Threat Prevention," National Security Agency, accessed January 12, 2022, https://www.nsa.gov/portals/75/documents/resources/everyone/csfc/threat-prevention.pdf.

214 House of Representatives, *Unauthorized Disclosures of Edward Snowden*.

215 House of Representatives.

- System Security Plans are often inaccurate or incomplete
- Two-person access (TPA) controls are not properly implemented for data centers and equipment rooms
- Removable media are not properly scanned for viruses.[216]

Another common finding was that employees had open access to bases and facilities. In contrast, members of the public would have to seek special permission to enter the base and even be screened by security. The Navy cannot advise whether more frequent inspections of personnel would have led to the discovery of Alexis's weapon before the shooting rampage.[217]

A common factor in each critical incident was the systematic failure of coworkers and supervisors to adequately address and document inappropriate behavior within the workplace for fear of hurting potential promotions or clearance status. That failure to follow procedures negates the policies and regulations meant to protect the organization and its personnel. The lack of reporting on all ends singlehandedly defeats the protocols designed to protect the agency.

C. CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE

In 2007, the UK's National Infrastructure Security Co-ordination Centre and the National Security Advice Centre combined their missions to create the CPNI.[218] The CPNI is the British government's national technical authority for physical and personnel protective security, charged with reducing vulnerability to insider threats to the UK and its essential infrastructure, as well as protecting against terrorism, espionage, and sabotage.[219] All organizations, private or public, rely on the CPNI for insider threat tools, best practices, and guidance.

---

216 Christopher Burgess, "NSA's Insider Threat Program Shows Shortcomings," Clearance Jobs, July 24, 2019, https://news.clearancejobs.com/2019/07/23/nsas-insider-threat-program-shows-shortcomings/.

217 Department of Defense, *Internal Review of the Washington Navy Yard Shooting*.

218 "Centre for the Protection of National Infrastructure (CPNI) Website," National Archives, accessed December 27, 2022, https://discovery.nationalarchives.gov.uk/details/r/C18403.

219 "Home Page," Centre for the Protection of National Infrastructure, accessed August 29, 2021, https://www.cpni.gov.uk.

The CPNI is an organization under MI5, the UK's national security agency. The CPNI does not make its personnel and organizational structure readily available, but as a child agency to MI5, a portion of its employees are dedicated to MI5 while others may be loaned out to other government agencies.[220] The CPNI works closely with other government departments, private businesses and organizations, academia, and security specialists, including the police.[221]

1. Policies

The CPNI advocates that all organizations vet every employee, including contractors, to the same standard. Contractors regularly have the same access to agency spaces and information as civilian employees.[222] The CPNI realizes that any worker has the potential to be an insider threat. Contractors' commitment to an organization's security culture and loyalty to the organization may not be as strong as civilian employees. Furthermore, it is common for organizations to circumvent security standards for contractors because some work from contract to contract and with different departments in the organization.[223]

The CPNI recommends several policies to disrupt hostile reconnaissance. As defined by the National Counter Terrorism Security Office, *hostile reconnaissance* is "the information-gathering phase conducted by those individuals or groups with malicious intent."[224] Disruptions can prevent a potential insider threat from gaining access to the sensitive data required to hurt the organization, increasing the potential for discovering an

220 "People and Organisation," MI5, accessed November 28, 2021, https://www.mi5.gov.uk/people-and-organisation.

221 "Who We Work With," Centre for the Protection of National Infrastructure, accessed November 28, 2021, https://www.cpni.gov.uk/who-we-work.

222 "Contract Staff," Centre for the Protection of National Infrastructure, accessed August 18, 2021, https://www.cpni.gov.uk/contract-staff.

223 Centre for the Protection of National Infrastructure.

224 "Guidance: Hostile Reconnaissance," UK National Counter Terrorism Security Office, November 2, 2020, https://www.gov.uk/government/publications/crowded-places-guidance/hostile-reconnaissance.

insider threat.[225] One method of disrupting hostile reconnaissance is *deterrence*, which the CPNI defines as "the intelligent, coordinated promotion of protective security provision to the hostile that results in the perception and/or assessment that the reconnaissance or the attack itself will fail."[226]

Another policy that the CPNI promotes is pre-employment screening, which is standard for most employers. In particular, the CPNI advocates a robust approach to standard criminal record checks, including an investigation of overseas records. Such an investigation includes a search for any criminal record while visiting or residing overseas and verifying overseas activities, including vacations, educational endeavors, employment, or anything else that might be an employment concern but would not appear on the applicant's domestic criminal record. This additional information allows each organization to adjudicate applicants and deny potential threats.[227]

The CPNI advocates organizations' maintaining a policy of transparency with their personnel on insider threat and privacy policies and organizational culture and values.[228] Organizations should widely educate, communicate, and publicize their views on acceptable behavior in and outside the workplace, including on social media.[229] These policies can help reduce the incidence of accidental insider threats and may deter intentional ones. These policies and repercussions for violating them should be taught during employee onboarding and reinforced periodically. They should stress proper information security, and employees should remain accountable to them outside of

225 "Disrupting Hostile Reconnaissance," Centre for the Protection of National Infrastructure, September 9, 2021, https://www.cpni.gov.uk/disrupting-hostile-reconnaissance-0.

226 "Deterrence," Centre for the Protection of National Infrastructure, September 21, 2020, https://www.cpni.gov.uk/deterrence.

227 Security Watchdog, *How to Obtain an Overseas Criminal Record Check: Quick Reference Guide* (Basingstoke, UK: Security Watchdog, 2018), https://www.cpni.gov.uk/system/files/documents/eb/21/How_to_Obtain_an_Overseas_Criminal_Record_Check_Quick_Reference_Guide_May_2018.pdf.

228 PA Consulting Group, *Holistic Management of Employee Risk (HoMER)* (London: PA Consulting Group, 2012), 12.

229 PA Consulting Group, 37.

work.[230] Creating a proactive security culture relies on buy-in from senior and middle management down to line employees.[231] This method is ideal for preventing insider threats rather than relying on detection after negative actions have already been taken.[232]

The CPNI promotes two pieces of legislation for organizations. First, the Data Protection Act of 1998 requires organizations to legally obtain and process all personal data collected.[233] Second, the Regulation of Investigatory Powers Act of 2000 regulates government agencies' surveillance and investigations along with their interception of internet activity and general telecommunications.[234] Ultimately, combating insider threats' illegal actions must not be performed with unregulated or illegal acts.

2. Procedures

The CPNI recommends completing an investigation upon any suspicion or occurrence of an insider threat. The assigned investigator, either an internal manager or outside organization, must be unbiased and obtain only the facts of the matter. It is imperative that the investigation be fair when dealing with witnesses or the subject of investigation, and the investigation must be factual if and when the subject has a hearing. If the subject feels the investigation was unfair or inaccurate, it could increase the risk of an insider threat in the future.[235]

Programs that bolster security measures tend to discourage an employee from causing harm to the organization or leaking sensitive information. However, a single program may not dissuade a potential insider threat, so multifaceted or integrated programs are more effective. To aid in this integration, the CPNI provides an insider risk mitigation

230 Centre for the Protection of National Infrastructure, *Investigating Employees of Concern: A Good Practice Guide* (London: Centre for the Protection of National Infrastructure, 2011), https://www.cpni.gov.uk/system/files/documents/d5/81/investigating-employees-of-concern.pdf.

231 "Personnel Security: An Ongoing Responsibility," Centre for the Protection of National Infrastructure, 2015, https://www.cpni.gov.uk/system/files/documents/5b/04/ongoing-personnel-security-infographic.pdf.

232 Centre for the Protection of National Infrastructure.

233 PA Consulting Group, *Holistic Management of Employee Risk*, 26.

234 PA Consulting Group, 26.

235 Centre for the Protection of National Infrastructure, *Investigating Employees of Concern*.

framework for organizations to guide their programs. Each organization can adopt this framework's foundation, implanting mitigations and concurrent actions to fit its budget and risk assessments. This framework can be used to bolster current insider threat programs.[236]

The CPNI promotes both behavior detection and insider risk models for a well-rounded program. Behavior detection, whereby employees' behavior is observed for any hostile intentions, is part of a robust, multifaceted approach to defend against insider threats.[237] For example, the CPNI developed the Passengers Assessment Screening System, utilized in London area airports, as a tool for behavior detection of passengers in addition to the current security screening process.[238] Organizational insider risk models focus on employees and their access to assets and information, in turn saving organizations money and allowing them to focus their resources on the subsequent cyber, physical, or human threat. This insider risk model also evaluates the organization's current insider threat countermeasures and assists in developing new measures to counter or reduce any threats from insiders (see Figure 2).[239]

236 "Insider Risk Mitigation Framework," Centre for the Protection of National Infrastructure, September 6, 2021, https://www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework.

237 "Behavioural Detection," Centre for the Protection of National Infrastructure, December 14, 2020, https://www.cpni.gov.uk/behavioural-detection-0.

238 María Carmen Feijoo-Fernández, Lucía Halty, and Andrés Sotoca-Plaza, "Like a Cat on Hot Bricks: The Detection of Anomalous Behavior in Airports," *Journal of Police and Criminal Psychology* (2020), https://doi.org/10.1007/s11896-020-09371-5.

239 "Insider Risk Assessment," Centre for the Protection of National Infrastructure, December 14, 2020, https://www.cpni.gov.uk/insider-risk-assessment.

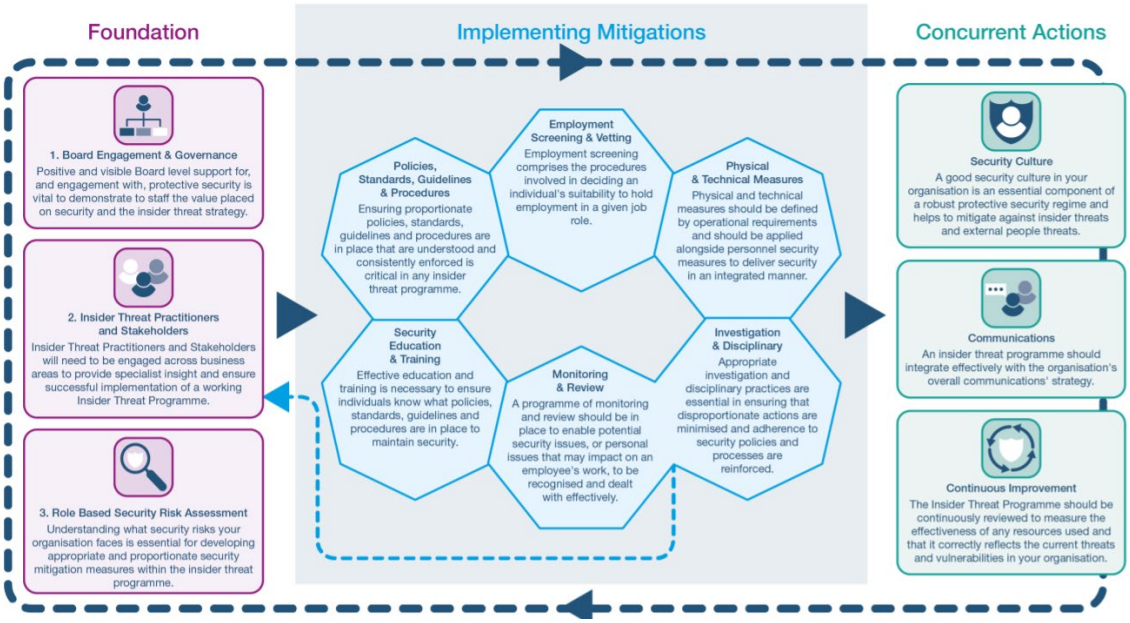

Figure 2. Insider Risk Mitigation Framework.[240]

Holistic Management of Employee Risk (HoMER) is another program that guides organizations in handling potential harm from an insider threat.[241] HoMER requires managers to engage in a holistic management style, which seeks input from all parts of the agency, preventing a siloed approach to insider threats. This input increases the effectiveness of addressing insider threats by allowing an organization to understand its culture and values wholly.[242] It emphasizes management's leading by example and setting the tone and expectations for the organization as a whole. For example, senior leaders who fail to wear their work badges would set a bad precedent and undermine security.[243]

[240] Source: "Insider Risk Mitigation Framework," Centre for the Protection of National Infrastructure, accessed December 5, 2021, https://www.cpni.gov.uk/sites/default/files/CPNI%20Insider%20Risk%20Mitigation%20Framework%20diagram%20accessible.pdf.

[241] PA Consulting Group, *Holistic Management of Employee Risk*.

[242] PA Consulting Group, 12.

[243] PA Consulting Group, 12.

3. Technologies

The CPNI has deemed access control technologies crucial to reducing potential insider threats. Organizations can utilize various levels of access control to tailor their risk tolerance appropriately.[244] One such technology comprises identity and access management tools, which can use multiple databases for different locations or other organizational assets. A primary challenge to deploying such a technology is that access control databases often lack synchronization or communication across platforms. Therefore, the CPNI recommends that organizations condense their databases and utilize a master database that is consistently updated.[245]

The CPNI recommends that behavior detection be integrated into a systematic security approach to mitigating insider threats. Behavior detection would be a collateral duty for employees, so it would not increase costs or necessitate hiring more personnel. This dynamic program requires the constant application of behavioral detection skills, technologies, and evidence-based training tailored to the organization.[246]

The former National Policing Improvement Agency (NIPA), a public organization that disseminated guidance on IT and information-sharing, acknowledged that data protection is an overwhelming domain to manage.[247] The technologies used to protect data can be easily defeated or circumvented by authorized users within the organization. The UK is not immune to insider threats from all sectors. The following sections illustrate that the UK's insider threats are not far off from those of the United States.

---

[244] PA Consulting Group, 31.

[245] PA Consulting Group, 32.

[246] Her Majesty's Government, *Behavioral Detection: Best Practice, Guidance, and Advice* (London: Her Majesty's Government, 2020), https://www.cpni.gov.uk/system/files/documents/03/73/CPNI0068_Behavioural_Detection_Brochure_DIGITAL_V8.pdf.

[247] UK National Policing Improvement Agency, *Annual Report and Accounts 2012/13* (London: Stationery Office, 2013), https://www.gov.uk/government/publications/national-policing-improvement-agency-annual-report-and-accounts-2012-to-2013.

4. Critical Incident 1: Data Breaches

In 2020, the UK's police force fell victim to more than 2,300 insider data breaches including unintentional insider threats and the willing misuse of police databases by employees.[248] Within the last five years, each police station has experienced nearly 300 data breaches on average. The data breaches were caused primarily by preventable employee errors from not following policy, for example, police employees emailing sensitive information to incorrect addressees and intentionally misusing police computers. Malicious cyberattacks from outside persons or organizations also accounted for a portion of the incidents.[249] Various police departments lost sensitive data to malicious actors, who could use the data for further malicious attacks on personnel and stakeholders. These police departments were fined thousands of British pounds for the breaches, and numerous police department employees were disciplined and terminated.[250]

Seba and Rowley's case study argues that the UK's police lack proper data-sharing policies. Specifically, police agencies in the UK understand the importance of proper, safe information-sharing, yet they experience difficulties in developing training for and overcoming cultural barriers to such practices.[251] Data breaches may not be completely preventable, but proper training and culture can help reduce them.

5. Critical Incident 2: British Airways Terrorism Plot

In February 2011, Rajib Karim was found guilty on multiple charges of terrorism, including plotting to blow up a plane. He had been an IT expert for British Airways and used his position and access to help organize the plot.[252] Before he planned to blow up the plane, Karim had explored a number of ways to wreak havoc, including accessing British

248 Phil Muncaster, "UK Police Suffered Thousands of Data Breaches in 2020," *Infosecurity Magazine*, May 26, 2021, https://www.infosecurity-magazine.com/news/uk-police-suffered-thousands-data/.

249 Muncaster.

250 Muncaster.

251 Ibrahim Seba and Jennifer Rowley, "Knowledge Management in UK Police Forces," *Journal of Knowledge Management* 14, no. 4 (2010): 611–26, https://doi.org/10.1108/13673271011059554.

252 Vikram Dodd, "British Airways Worker Rajib Karim Convicted of Terrorist Plot," *Guardian*, February 28, 2011, https://www.theguardian.com/uk/2011/feb/28/british-airways-bomb-guilty-karim.

Airlines' servers and deleting all of the data and joining a cabin crew to cover for striking colleagues.[253] Throughout these plans, he sent encrypted messages to his partner and brother. Karim strategically avoided the collection of metadata from his computer to circumvent detection.[254] In fact, the encryption used by Karim was described by British Airways police "as the most sophisticated they had seen in a British terrorist case."[255]

Rajib Karim is an example of how even layered approaches to insider threat detection could fail. The authorities believe Karim to be a violent jihadist who accepted the position with British Airways with violent intent.[256] He also evaded technologies intended to monitor passively for threats. Karim used both software and social engineering to take advantage of loopholes present in the insider threat framework.

6. Key Findings

Each critical incident for these UK-based organizations could have been prevented or avoided as each organization can access the CPNI's products and policies, and such insider actions are common events around the globe. As a federalized department, the UK police have often lacked a proper and immediate response to insider threats through training, education, and disciplinary action against employees violating data privacy policies. With an average of six insider data breaches daily, the UK police have failed to address the problem.[257] British Airways may have been sabotaged by an employee. Its announcement of layoffs may have been the catalyst for sabotaging the planes, despite providing employees with access to a well-being team for any mental or emotional assistance they need. These organizations do not reflect critically on the CPNI, as the CPNI, much like TSA, offers resources through products and education that could greatly benefit each organization.

---

253 Steve Swann, "Rajib Karim: The Terrorist inside British Airways," BBC News, February 28, 2011, https://www.bbc.com/news/uk-12573824.

254 Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel* 9, no. 6 (June 2016), https://ctc.westpoint.edu/how-terrorists-use-encryption/.

255 Dodd, "British Airways Worker Rajib Karim Convicted of Terrorist Plot," para. 7.

256 Dodd.

257 Muncaster, "UK Police Suffered Thousands of Data Breaches in 2020."

The UK's agencies understand that their organizations alone cannot combat or prevent all insider threats that might disseminate sensitive classified information, hinder economic participation, or otherwise cause harm. MI5, the UK's security service; the Secret Intelligence Service; and the Government Communications Headquarters work together to prevent, deter, and capture insider threats at the government level. These organizations also partner with other government departments in the UK, including the police, when warranted.

D. CONCLUSION

In summary, this chapter has examined and compared how three government agencies assess and mitigate insider threats via screening, policies, and procedures. These agencies understand the importance of protecting their organizations from the inside out. Their methods for mitigating and detecting insider threats vary significantly in implementation and effectiveness; however, the consensus is that insider threats are a tangible danger that needs to be addressed. The next chapter provides conclusions and recommendations from all the organizations analyzed.

V. RECOMMENDATIONS AND CONCLUSION

Overall, this thesis presented a thorough review of insider threats that can harm federal organizations. Chapter I of this thesis introduced the topic of insider threats, specifically regarding their effect on TSA. It demonstrated that insider threats are a serious issue, citing previous insider actions that harmed the transportation sector specifically. The literature review in Chapter II presented various organizations' definitions of insider threat, showed the increasing risk of insider threats and methods of threat detection. While there were gaps in the literature, numerous scholars and practitioners agree on the need for continuous insider threat detection. Chapter III provided an overview of TSA's ITP, including screening procedures of current TSA employees. Among the key findings of this chapter were the inconsistent screening processes for certain employees with sensitive access, a lack of screening beyond the initial pre-employment process, and the need to adopt passenger screening technologies to internal employee screening. Chapter IV offered an extensive comparative analysis of the FBI's, DOD's, and CPNI's ITPs.

This chapter provides recommendations for TSA based on the insider threat detection and prevention methods and respective critical incidents of the FBI, DOD, and CPNI. While there is no silver bullet for combating insider threats, and each organization has a diverse employee population, TSA can take additional steps to further protect the agency and the traveling public.

A. RECOMMENDATIONS

1. Pre-employment Screening

TSA should oversee a standardized pre-employment screening of 100 percent of all transportation workers before onboarding. There is ample evidence to suggest that pre-employment screening potentially prevents a threat from becoming an insider. Just as the CPNI is the UK's central point of contact for all organizations to establish, mold, and maintain their insider threat programs, TSA needs to become that lynchpin for the transportation sector in the United States. TSA programs currently in place, such as the TWIC required to access secure areas in maritime facilities and vessels, should be

expanded to every transportation sector.[258] Similarly, the screening process for the SIDA badge—used to access secure areas in airports and offered only to a limited population—should be administered to all airport employees. While it would not be feasible or cost effective for TSA to undertake the screening of all transportation sector employees, the private organizations that employ transportation workers should be required to adopt and maintain TSA's standards for employment. The OPM; the DCSA; and airline, maritime, and surface industries would need to start a working group and create a solution for undertaking this recommendation. TSA's proprietary access to its databases could further assist with this recommendation to standardize or oversee pre-employment vetting for all transportation employees.

2. Periodic Screening

TSA should enact random and periodic screenings of all TSA employees. The CPNI found that of all uncovered insider threats, 76 percent became threats only after joining their organization.[259] Currently, participation in any proactive insider threat initiatives is strictly voluntary at TSA, and TSA employees and airport workers are not continuously vetted throughout their careers. This workforce could be recruited as insider threats before employment with TSA or after employment is granted. Traditionally, transportation security officers and most airport employees are not paid competitively, and these positions pose relatively low barriers to entry. Such factors may enable a nefarious actor to infiltrate the TSA or the transportation sector. A bad actor could also coerce, entice, or bribe a current officer or aviation employee to engage in terrorism; sabotage; or smuggling of persons, weapons, drugs, or other contraband. It is in TSA's best interest to create an initiative that engages all current employees in random screening with the possibility of a polygraph.

A key resource for accomplishing this recommendation would be TSA Investigations (INV), specifically the special agents who are federally certified, TSA-

[258] Transportation Security Administration, "TWIC."

[259] 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).

designated polygraph examiners. The airports would need to increase manning and pay overtime to compensate employees for undergoing screening during work hours. The FBI and certain DOD agencies use this method for CE.

These measures would be expensive for the agency, taxpayers, and the flying public. Adopting this continuous vetting standard would be a vast undertaking requiring policy and legal changes and an increase in manning, resources, and specially trained polygraph examiners (civilians or contractors). The attrition rate of staff would increase as TSA would lose a percentage of its workforce when random background checks and polygraphs were implemented due to the derogatory information obtained.

3. Partnerships

TSA should leverage partnerships to advance insider threat detection. Both the CPNI and DOD utilize partnerships to increase their capacity and the reach of their insider threat mitigation strategies. TSA could implement several partnership tactics. First, as an agency housed under DHS—an umbrella organization comprising numerous other law enforcement agencies with vast human, financial, and technological resources—TSA could identify mutually beneficial strategies to leverage these resources to help reduce insider threats across DHS. Second, TSA should consider partnerships as a strategy to avoid conflicts of interest and ensure impartiality. For example, a memorandum of understanding could be established with the Customs and Border Protection's Office of Professional Responsibility to assist with polygraphs for internal investigations of TSA's INV personnel and for situations when a TSA INV examiner would polygraph a senior leader for the other's supervisory chain of command.

4. Criminal Investigators

TSA should hire designated criminal investigators tasked specifically with investigating insider threats within TSA. Both the FBI and DOD have created specialized teams as a part of their insider threat mitigation strategies. These teams serve as designated experts who are consulted in a collaborative and comprehensive program. TSA INV investigates criminal misconduct, threats to TSA and the transportation system, and employee misconduct. TSA INV is already short-staffed, and most of its agents are tasked

with running multiple investigations along with their other duties, such as polygraphs and technical services such as computer forensics and technical and clandestine surveillance. TSA INV's Technical Services Branch (TSB) would be best suited to handle insider threat investigations affecting TSA. As a dedicated staff of special agents all over the country who can focus specifically on insider threats, TSB agents are well versed in counterintelligence issues, have arrest authority, and can greatly improve the efficiency of TSA's ITP. TSB agents are generally free from administrative or criminal investigations in a particular region. A designated legal counsel with real-world experience litigating criminal cases should also be embedded within TSA INV's insider threat unit, running these investigations independently or, building from Recommendation 3, working jointly with the FBI. TSA must remain committed to developing and implementing the roadmap as it contains the critical elements of a strategic plan to keep its ITP at the forefront of detection and mitigation.

B. ADDITIONAL RESEARCH NEEDED

A number of gaps in understanding the impacts of insider threat detection and prevention at the federal level would benefit from further research. First, this research included only publicly available and open-source information due to the sensitivity of the topic. Incorporating other data sources may yield additional methodologies, challenges, and recommendations. Second, as discussed previously, continuous or random vetting of all aviation employees will better protect TSA from employees' becoming insider threats after being hired. Additional research is needed on TSA's authority and the legality of extensively vetting new and current employees. Third, more work is needed to develop robust strategies that demonstrate the impact and effectiveness of insider threat mitigation tactics. Although they would be difficult to conduct, longer-term studies to quantify the impact of a layered insider threat detection approach would benefit this area of practice. Last, research to carry out a cost–benefit analysis of expanding insider threat detection capabilities would be beneficial.

C. CONCLUSION

TSA is critical to keeping the traveling public safe through various tactics, including passenger and cargo screening and other aviation security channels. Domestic extremism and violence, rather than foreign terrorism, are quickly morphing into TSA's greatest threat. The best way to protect TSA and the flying public is by thoroughly and continuously vetting all applicants and current aviation employees by mimicking the DOD's and FBI's personnel security procedures and looking to best practices implemented internationally, like those of the CPNI. TSA will face hurdles in undertaking these policy changes, but TSA's current policy lacks the procedures and requirements to be effective.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Aftergood, Steven. "DOD Adds 'Credibility Assessment' to Polygraph Program." *Federation of American Scientists* (blog), February 12, 2007. https://fas.org/blogs/secrecy/2007/02/dod_adds_credibility_assessmen/.

Al-Mhiqani, Mohammed Nasser, Rabiah Ahmad, Z. Zainal Abidin, Warusia Yassin, Aslinda Hassan, Karrar Hameed Abdulkareem, Nabeel Salih Ali, and Zahri Yunos. "A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations." *Applied Sciences* 10, no. 15 (January 2020): 5208. https://doi.org/10.3390/app10155208.

ASIS International. *Risk Assessment*. Vol. 1. Alexandria, VA: ASIS International, 2015. http://www.asisonline.org/publications--resources/standards--guidelines/ra/annex-c/.

Barrios, Rita M. "A Multi-Leveled Approach to Intrusion Detection and the Insider Threat." *Journal of Information Security* 4, no. 1 (2013): 54–65. https://doi.org/10.4236/jis.2013.41007.

Baweja, Jessica A., Shannen M. McGrath, Danielle L. Burchett, and Stephanie L. Jaros. *An Evaluation of the Utility of Expanding Psychological Screening to Prevent Insider Attacks*. OPA Report No. 2019–067. Seaside, CA: Defense Personnel and Security Research Center, Office of People Analytics, 2019. https://apps.dtic.mil/sti/citations/AD1083812.

Becker, Andrew. "Viagra-Smuggling Scandal Hits Federal Air Marshals." Yahoo, December 22, 2020. https://www.yahoo.com/now/viagrasmuggling-scandal-hits-federal-air-marshals-155928349.html.

Burgess, Christopher. "NSA's Insider Threat Program Shows Shortcomings." Clearance Jobs, July 24, 2019. https://news.clearancejobs.com/2019/07/23/nsas-insider-threat-program-shows-shortcomings/.

Center for Development of Security Excellence. *DOD Insider Threat Management Analysis Center (DITMAC) Short Student Guide*. Linthicum Heights, MD: Center for Development of Security Excellence, 2016. https://www.cdse.edu/Portals/124/Documents/student-guides/shorts/INT100-guide.pdf.

———. *Introduction to Personnel Security: Student Guide*. PS113.16. Linthicum Heights, MD: Center for Development of Security Excellence, 2020. https://www.cdse.edu/documents/student-guides/PS113-guide.pdf.

———. “Shamai Leibowitz Case Study: Unauthorized Disclosure.” Accessed September 27, 2021. https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-shamai-leibowitz.pdf.

Centre for the Protection of National Infrastructure. “Behavioural Detection.” December 14, 2020. https://www.cpni.gov.uk/behavioural-detection-0.

———. “Contract Staff.” Accessed August 18, 2021. https://www.cpni.gov.uk/contract-staff.

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

———. “Deterrence.” September 21, 2020. https://www.cpni.gov.uk/deterrence.

———. “Disrupting Hostile Reconnaissance.” September 9, 2021. https://www.cpni.gov.uk/disrupting-hostile-reconnaissance-0.

———. “Home Page.” Accessed August 29, 2021. https://www.cpni.gov.uk.

———. “Insider Risk Assessment.” December 14, 2020. https://www.cpni.gov.uk/insider-risk-assessment.

———. “Insider Risk Mitigation Framework.” September 6, 2021. https://www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework.

———. “Insider Risk Mitigation Framework.” Accessed December 5, 2021. https://www.cpni.gov.uk/sites/default/files/CPNI%20Insider%20Risk%20Mitigation%20Framework%20diagram%20accessible.pdf.

———. *Investigating Employees of Concern: A Good Practice Guide*. London: Centre for the Protection of National Infrastructure, 2011. https://www.cpni.gov.uk/system/files/documents/d5/81/investigating-employees-of-concern.pdf.

———. “Personnel Security: An Ongoing Responsibility.” 2015. https://www.cpni.gov.uk/system/files/documents/5b/04/ongoing-personnel-security-infographic.pdf.

———. “Reducing Insider Risk.” May 25, 2021. https://www.cpni.gov.uk/reducing-insider-risk.

———. “Who We Work With.” Accessed November 28, 2021. https://www.cpni.gov.uk/who-we-work.

Cherdantseva, Yulia, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. “A Review of Cyber Security Risk Assessment Methods for SCADA Systems.” *Computers & Security* 56 (February 2016): 1–27. https://doi.org/10.1016/j.cose.2015.09.009.

CyLumena. “Why Take a Risk-Based (Instead of Compliance) Approach to Cybersecurity.” Accessed August 22, 2021. https://www.cylumena.com/insights/risk-based-cybersecurity/.

Czarnecki, Fabrice. *Medical & Psychological Guidelines for Transportation Security Officers*. Washington, DC: Transportation Security Administration, 2018. https://jobs.tsa.gov/Resources/TSO_Medical_Guidelines.pdf.

Defense Counterintelligence and Security Agency. “About Us.” Accessed August 14, 2022. https://www.dcsa.mil/About/.

———. “Investigations, Adjudications and Clearance Processes at a Glance.” Accessed November 25, 2021. https://www.dcsa.mil/mc/pv/mbi/gicp/.

DelBene, Kurt, Milo Medin, and Richard Murray. *The Road to Zero Trust (Security)*. Washington, DC: Defense Innovation Board, 2019. https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_%28SECURITY%29_07.08.2019.PDF.

Denson, Bryan. “How Financial Triggers Can Help Spot Insider Threats.” GCN, August 5, 2020. https://gcn.com/cybersecurity/2020/08/how-financial-triggers-can-help-spot-insider-threats/315135/.

Department of Defense. “About.” Accessed October 13, 2021. https://www.defense.gov/About/.

———. *The DOD Insider Threat Program*. DOD Directive 5205.16. Washington, DC: Department of Defense, 2017. https://irp.fas.org/doddir/dod/d5205_16.pdf.

———. *DOD Physical Fitness and Body Fat Programs Procedures*. DOD Instruction 1308.3. Washington, DC: Department of Defense, 2002. https://biotech.law.lsu.edu/blaw/dodd/corres/html/13083.htm.

———. *Internal Review of the Washington Navy Yard Shooting*. Washington, DC: Department of Defense, 2013. https://permanent.fdlp.gov/gpo46879/DOD-Internal-Review-of-the-WNY-Shooting-20-Nov-2013.pdf.

———. *Medical Standards for Military Service: Appointment, Enlistment, or Induction*. DOD Instruction 6130.03. Vol. 1. Washington, DC: Department of Defense, 2021.

———. *Zero Trust Reference Architecture*. Washington, DC: Department of Defense, 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

Department of Homeland Security. *FY 2022 Budget in Brief*. Washington, DC: Department of Homeland Security, 2021. https://www.dhs.gov/sites/default/files/publications/dhs_bib_-_web_version_-_final_508.pdf.

———. *Transportation Security Administration Budget Overview: Fiscal Year 2023 Congressional Justification*. Washington, DC: Department of Homeland Security, 2022. https://www.dhs.gov/sites/default/files/2022-03/Transportation%20Security%20Administration_Remediated.pdf.

Department of Homeland Security, Office of Inspector General. *Transportation Security Administration Has Taken Steps to Address the Insider Threat but Challenges Remain (Redacted)*. OIG-12-120. Washington, DC: Department of Homeland Security, Office of Inspector General, 2012. https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/2012/OIGr_12-120_Sep12.pdf.

Department of Justice. "Former FBI Contract Linguist Pleads Guilty to Leaking Classified Information to Blogger." December 17, 2009. https://www.justice.gov/opa/pr/former-fbi-contract-linguist-pleads-guilty-leaking-classified-information-blogger.

Department of Justice, Office of the Inspector General. *Public Summary: Audit of the Federal Bureau of Investigation's Insider Threat Program*. Washington, DC: Department of Justice, Office of the Inspector General, 2017. https://sgp.fas.org/othergov/dojig-itp.pdf.

———. "Review of FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen." August 14, 2003. https://irp.fas.org/agency/doj/oig/hanssen.html.

Dice. "Insider Threats: Why These Cybersecurity Incidents Continue to Grow." February 21, 2022. https://www.dice.com/career-advice/insider-threats-why-these-cybersecurity-incidents-continue-to-grow.

Dodd, Vikram. "British Airways Worker Rajib Karim Convicted of Terrorist Plot." *Guardian*, February 28, 2011. https://www.theguardian.com/uk/2011/feb/28/british-airways-bomb-guilty-karim.

Ebersole, Kyle. "Continuous Evaluation: Welcoming Government Employees to the World of Mass Surveillance." *George Mason Law Review* 23, no. 2 (2016): 445–77.

Edwards, Scott. "The Psychological Evaluation and Your Security Clearance: Why You Shouldn't Overshare." Clearance Jobs, November 22, 2020. https://news.clearancejobs.com/2020/11/22/the-psychological-evaluation-and-your-security-clearance-oversharing-can-ruin-your-career/.

Elifoglu, I. Hilmi, Ivan Abel, and Özlem Taşseven. "Minimizing Insider Threat Risk with Behavioral Monitoring." *Review of Business: Interdisciplinary Journal on Risk and Society* 38, no. 2 (2018): 61–73. https://www.stjohns.edu/sites/default/files/uploads/review-of-business-382-june_2018.pdf.

Federal Bureau of Investigation. "Background Checks for New Applicants." In *Inside the FBI*, April 17, 2009. Podcast, MP3 audio, 6:48. https://www.fbi.gov/audio-repository/news-podcasts-inside-background-checks-for-new-applicants.mp3/view.

———. "Brian P. Regan Espionage." Accessed June 6, 2022. https://www.fbi.gov/history/famous-cases/brian-p-regan-espionage.

———. "Mission & Priorities." Accessed October 7, 2021. https://www.fbi.gov/about/mission.

———. *Personnel Security Clearance and Access Policy Guide*. Washington, DC: Federal Bureau of Investigation, 2009. https://vault.fbi.gov/personnel-security-clearance-and-access-policy-guide-0192pg/personnel-security-clearance-and-access-policy-guide-0192pg-part-01-of-01.

Feijoo-Fernández, María Carmen, Lucía Halty, and Andrés Sotoca-Plaza. "Like a Cat on Hot Bricks: The Detection of Anomalous Behavior in Airports." *Journal of Police and Criminal Psychology* (2020). https://doi.org/10.1007/s11896-020-09371-5.

Galbraith, Jay. "The Star Model." Galbraith Management Consultants. Accessed May 11, 2021. https://www.jaygalbraith.com/images/pdfs/StarModel.pdf.

Goldstein, Harry. "Who Killed the Virtual Case File?" *IEEE Spectrum*, September 1, 2005. https://spectrum.ieee.org/who-killed-the-virtual-case-file.

Graham, Robert. "How Terrorists Use Encryption." *CTC Sentinel* 9, no. 6 (June 2016): 20–25. https://ctc.westpoint.edu/how-terrorists-use-encryption/.

Greitzer, Frank L. "Insider Threats: It's the Human, Stupid!" In *Proceedings of the Northwest Cybersecurity Symposium*, 1–8. New York: Association for Computing Machinery, 2019. https://doi.org/10.1145/3332448.3332458.

Her Majesty's Government. *Behavioral Detection: Best Practice, Guidance, and Advice*. London: Her Majesty's Government, 2020. https://www.cpni.gov.uk/system/files/documents/03/73/CPNI0068_Behavioural_Detection_Brochure_DIGITAL_V8.pdf.

Hill, Henry J. "Impact of Altering the Delinquent Debt Threshold Used for Background Investigation Expansion on the Denial Rate of Security Clearances." Master's thesis, Naval Postgraduate School, 1991. https://apps.dtic.mil/sti/pdfs/ADA247331.pdf.

Holden, Henry M. *To Be an FBI Special Agent*. St. Paul, MN: Zenith Press, 2005.

Gelles, Michael G. "How to Handle the Risk of Insider Threats Post-COVID-19." TechTarget, May 12, 2020. https://searchcio.techtarget.com/feature/How-to-handle-the-risk-of-insider-threats-post-COVID-19.

Grover, Jennifer. *Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates*. GAO-16-632. Washington, DC: Government Accountability Office, 2016. https://www.gao.gov/products/gao-16-632.

Hurd, Sandra N. "Use of the Polygraph in Screening Job Applicants." *American Business Law Journal* 22, no. 4 (Winter 1985): 529–49. ProQuest.

Intelligence and National Security Alliance, Insider Threat Task Force. *A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector*. Arlington, VA: Intelligence and National Security Alliance, 2013.

International Air Transportation Association. *Insider Threat in Civil Aviation*. Montreal: International Air Transportation Association, 2018. https://www.iata.org/contentassets/e55ae27b2fc34343a1143fca5129c8dd/insider-threats-position.pdf.

Jackson, Monica. "FBI Employs AI, Big Data Analytics Systems to Identify Insider Threats." ExecutiveGov, August 24, 2018. https://www.executivegov.com/2018/08/fbi-employs-ai-big-data-analytics-systems-to-identify-insider-threats/.

Jacobs, Jonathan B., and Louis F. Dell'Osso. "Congenital Nystagmus: Hypotheses for Its Genesis and Complex Waveforms within a Behavioral Ocular Motor System Model." *Journal of Vision* 4, no. 7 (July 2004): 604–25. https://doi.org/10.1167/4.7.7.

Kircher, John, and David Raskin. "Laboratory and Field Research on the Ocular-Motor Deception Test." *European Polygraph* 10, no. 4 (2016): 160–72. https://doi.org/10.1515/ep-2016-0021.

Kramer, Lisa A., and Richards J. Heuer Jr. "America's Increased Vulnerability to Insider Espionage." *International Journal of Intelligence and CounterIntelligence* 20, no. 1 (2007): 50–64. https://doi.org/10.1080/08850600600888698.

Krow, Shailynn. "Military Recruiter Job Responsibilities." *Houston Chronicle*. Accessed November 22, 2021. https://work.chron.com/military-recruiter-job-responsibilities-12701.html.

Kurlychek, Megan C., Robert Brame, and Shawn D. Bushway. "Enduring Risk? Old Criminal Records and Predictions of Future Criminal Involvement." *Crime & Delinquency* 53, no. 1 (2007): 64–83. https://doi.org/10.1177/0011128706294439.

Lang, Eric L. *Security Background Investigations and Clearance Procedures of the Federal Government*. Management Report 05–5. Monterey, CA: Defense Personnel and Security Research Center, 2005. https://www.dhra.mil/Portals/52/Documents/perserec/mr05-05.pdf.

Larence, Eileen Regen. *Information Sharing Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities*. GAO-13-471. Washington, DC: Government Accountability Office, 2003. https://www.ojp.gov/pdffiles1/Digitization/203371NCJRS.pdf.

Lopez, C. Todd. "DOD Program Aims to Deter Insiders from Harmful Acts." Department of Defense, September 17, 2019. https://www.defense.gov/Explore/News/Article/Article/1962031/dod-program-aims-to-deter-insiders-from-harmful-acts/.

Luckey, David, David Stebbins, Rebeca Orrie, Erin Rebhan, Sunny Bhatt, and Sina Beaghley. *Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Posture of the U.S. Departments and Agencies Be Improved?* Santa Monica, CA: RAND Corporation, 2019. https://doi.org/10.7249/RR2684.

MacLaren, Vance. "Can We Trust Counterintelligence Polygraph Tests?" *Polygraph* 29, no. 2 (2000): 151–54. https://www.polygraph.org/assets/docs/APA-Journal.Articles/Vol.29.2000/polygraph%202000%20292.pdf#page=16.

McNeil, Triana. *Aviation Security: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals*. GAO-20-275. Washington, DC: Government Accountability Office, 2020. https://www.gao.gov/products/GAO-20-275.

Means, Barbara. *Moral Standards for Military Enlistment: Screening Procedures and Impact*. Alexandria, VA: Human Resources Research Organization,1983. https://apps.dtic.mil/sti/citations/ADA135995.

MI5. "People and Organisation." Accessed November 28, 2021. https://www.mi5.gov.uk/people-and-organisation.

Miller, Jason. "FBI Boosts IT Efforts to Protect Itself from Rogue Employees." Federal News Network, May 14, 2018. https://federalnewsnetwork.com/reporters-notebook-jason-miller/2018/05/fbi-boosts-it-efforts-to-protect-itself-from-rogue-employees/.

Mills, Robert F., Gilbert L. Peterson, and Michael R. Grimaila. "Insider Threat Prevention, Detection and Mitigation." In *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*, edited by Kenneth J. Knapp, 48–74. Hershey, PA: IGI Global, 2009. https://www.igi-global.com/chapter/insider-threat-prevention-detection-mitigation/7410.

Muncaster, Phil. "UK Police Suffered Thousands of Data Breaches in 2020." *Infosecurity Magazine*, May 26, 2021. https://www.infosecurity-magazine.com/news/uk-police-suffered-thousands-data/.

National Archive. "Centre for the Protection of National Infrastructure (CPNI) Website." Accessed December 27, 2022. https://discovery.nationalarchives.gov.uk/details/r/C18403.

National Security Agency. "Commercial Solutions for Classified (CSfC) Threat Prevention." Accessed January 12, 2022. https://www.nsa.gov/portals/75/documents/resources/everyone/csfc/threat-prevention.pdf.

Nelson, Raymond. "Scientific Basis for Polygraph Testing." *Polygraph* 44, no. 1 (2015): 28–61.

Office of the Director of National Intelligence. *Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications*. SEAD-5. Washington, DC: Office of the Director of National Intelligence, 2016. https://www.cdse.edu/documents/toolkits-personnel/SEAD-5.pdf.

———. "Members of the IC." Accessed November 22, 2021. https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

———. *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*. ICD 704. Washington, DC: Office of the Director of National Intelligence, 2008. https://www.hsdl.org/?abstract&did=234672.

PA Consulting Group. *Holistic Management of Employee Risk (HoMER)*. London: PA Consulting Group, 2012.

Phalen, Charles. "Statement before the Subcommittee on Government Operations, House Oversight and Government Reform Committee, United States House of Representatives." Washington, DC: Office of Personnel Management, 2017. https://www.opm.gov/news/testimony/115th-congress/nbib-director-charles-phalen-testimony-before-hogr-govt-operations-subcommittee.pdf.

Rice, Harvey. "Air Marshals Charged in Cocaine Smuggling Plot." *Houston Chronicle*, February 13, 2006. https://www.chron.com/news/houston-texas/article/Air-marshals-charged-in-cocaine-smuggling-plot-1897010.php.

Rose, Andrée E., David P. Prina, Melissa D. Palmer, and Brandon Rapoza. *Leveraging FBI Resources to Enhance Military Accessions Screening and Personnel Security Vetting*. OPA Report No. 2020–080-O. Seaside, CA: Defense Personnel and Security Research Center, 2020.

Rudner, Martin. "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge." *International Journal of Intelligence and CounterIntelligence* 26, no. 3 (September 2013): 453–81. https://doi.org/10.1080/08850607.2013.780552.

Russell, William. *Aviation Security: Federal Air Marshal Service Has Taken Steps to Address Workforce Issues, but Additional Actions Needed*. Washington, DC: Government Accountability Office, 2020. https://www.gao.gov/assets/gao-20-125.pdf.

Sackett, Paul R., and Anne S. Mavor, eds. *Assessing Fitness for Military Enlistment: Physical, Medical, and Mental Health Standards*. Washington, DC: National Academies Press, 2006. https://doi.org/10.17226/11511.

Schneider, Kristin G., Danielle L. Burchett, Catina M. Smith, Marie M. Osborn, Jennifer A. L. Vanberschot, and Rene M. Dickerhoof. *A Personnel Security Training Program for Clinicians: Phase III*. OPA Report No. 2020–002. Seaside, CA: Defense Personnel and Security Research Center, Office of People Analytics, 2019. https://apps.dtic.mil/sti/citations/AD1089287.

Schultz, E. Eugene. "A Framework for Understanding and Predicting Insider Attacks." *Computers & Security* 21, no. 6 (2002): 526–31. https://doi.org/10.1016/S0167-4048(02)01009-X.

Seba, Ibrahim, and Jennifer Rowley. "Knowledge Management in UK Police Forces." *Journal of Knowledge Management* 14, no. 4 (2010): 611–26. https://doi.org/10.1108/13673271011059554.

Security Watchdog. *How to Obtain an Overseas Criminal Record Check: Quick Reference Guide*. Basingstoke, UK: Security Watchdog, 2018. https://www.cpni.gov.uk/system/files/documents/eb/21/How_to_Obtain_an_Overseas_Criminal_Record_Check_Quick_Reference_Guide_May_2018.pdf.

Senser, Kenneth H. "Testimony before the Senate Judiciary Committee." Federal Bureau of Investigation, July 18, 2001. https://www.fbi.gov/news/testimony/review-of-the-fbi-security-program-and-its-transformation.

Spooner, Derrick, George Silowash, Daniel Costa, and Michael Albrethsen. "Navigating the Insider Threat Tool Landscape: Low Cost Technical Solutions to Jump Start an Insider Threat Program." In *2018 IEEE Security and Privacy Workshops*, 247–57. Piscataway, NJ: IEEE, 2018. https://doi.org/10.1109/SPW.2018.00040.

Swann, Steve. "Rajib Karim: The Terrorist inside British Airways." BBC News, February 28, 2011. https://www.bbc.com/news/uk-12573824.

Sweeney, Denis. "Social Media Screening of Homeland Security Job Applicants and the Implications on Free Speech Rights." Master's thesis, Naval Postgraduate School, 2019.

Taylor, Paul J., Coral J. Dando, Thomas C. Ormerod, Linden J. Ball, Marisa C. Jenkins, Alexandra Sandham, Tarek Menacere, Alexandra Sandham, and Tarek Menacere. "Detecting Insider Threats through Language Change." *Law and Human Behavior* 37, no. 4 (August 2013): 267–75. http://doi.org/10.1037/lhb0000032.

Toriello-Fite, Karen A. "Insider Threat Risk Assessment and Telework." Linthicum Heights, MD: Center for Development of Security Excellence, 2021.

Transportation Security Administration. "Emerging Technology." Accessed August 29, 2022. https://www.tsa.gov/travel/security-screening/emerging-technology.

———. *Enterprise Risk Management*. TSA Management Directive No. 100.8. Springfield, VA: Transportation Security Administration, 2014. https://www.tsa.gov/sites/default/files/foia-readingroom/enterprise_risk_management_100._8.pdf.

———. "For Industry." Accessed January 13, 2022. https://www.tsa.gov/for-industry.

———. *Insider Threat Program*. TSA Management Directive No. 2800.17. Springfield, VA: Transportation Security Administration, 2013. https://www.tsa.gov/sites/default/files/foia-readingroom/insider_threat_program_2800.17pdf.pdf.

———. *Insider Threat Roadmap 2020*. Springfield, VA: Transportation Security Administration, 2020. https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf.

———. "Law Enforcement." Accessed January 31, 2022. https://jobs.tsa.gov/law-enforcement.

———. "Mission." Accessed January 30, 2022. https://www.tsa.gov/about/tsa-mission.

———. "Risk-Based Security." Accessed August 29, 2022. https://www.tsa.gov/news/press/factsheets/risk-based-security.

———. *SIDA Airport Security: Fiscal Year 2017 Report to Congress*. Springfield, VA: Transportation Security Administration, 2018.

———. "TWIC." Accessed August 22, 2021. https://www.tsa.gov/for-industry/twic.

———. "Understanding the Federal Hiring Process." Accessed January 23, 2022. https://jobs.tsa.gov/federal-hiring-process.

UK National Counter Terrorism Security Office. "Guidance: Hostile Reconnaissance." November 2, 2020. https://www.gov.uk/government/publications/crowded-places-guidance/hostile-reconnaissance.

UK National Policing Improvement Agency. *Annual Report and Accounts 2012/13*. London: Stationery Office, 2013. https://www.gov.uk/government/publications/national-policing-improvement-agency-annual-report-and-accounts-2012-to-2013.

Urban Institute. "Five Problems with Criminal Background Checks." Accessed June 12, 2022. https://www.urban.org/urban-wire/five-problems-criminal-background-checks.

USA Jobs. "Special Agent – Law Enforcement or Military Veteran Background." Accessed October 30, 2021. https://www.usajobs.gov:443/GetJob/ViewDetails/463469600.

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

U.S. Congress. House of Representatives. *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden*. Washington, DC: House of Representatives, 2016. https://www.congress.gov/114/crpt/hrpt891/CRPT-114hrpt891.pdf.

U.S. Intelligence Community Careers. "Application Process." Accessed October 14, 2021. https://www.intelligencecareers.gov/application-process.

U.S. Northern Command. "About." Accessed November 22, 2021. https://www.northcom.mil/About-USNORTHCOM/.

von Solms, Sune, and Renier van Heerden. "The Consequences of Edward Snowden NSA Related Information Disclosures." In *Proceedings of the 10th International Conference on Cyber Warfare and Security*. Reading, UK: Academic Conferences and Publishing International, 2015.

Wasko, Shannon, Rebecca E. Rhodes, Megan Goforth, Nathan Bos, Hannah P. Cowley, Gerald Matthews, Alice Leung, Satish Iyengar, and Jonathon Kopecky. "Using Alternate Reality Games to Find a Needle in a Haystack: An Approach for Testing Insider Threat Detection Methods." *Computers & Security* 107 (2021). https://doi.org/10.1016/j.cose.2021.102314.

Wilshusen, Gregory C., and Nabajyoti Barkakati. *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*. GAO-17-614. Washington, DC: Government Accountability Office, 2017. https://www.gao.gov/assets/gao-17-614.pdf.

Workplace Testing. "What Is a Criminal Record Check?" May 29, 2020. http://www.workplacetesting.com/definition/710/criminal-record-check.

Yaseen, Qussai, and Brajendra Panda. "Insider Threat Mitigation: Preventing Unauthorized Knowledge Acquisition." *International Journal of Information Security* 11, no. 4 (August 2012): 269–80. http://dx.doi.org/10.1007/s10207-012-0165-6.

Young, Sarah. "Continuous Evaluation: Background Investigations, Classified Information, and Informing in the 21st Century." Illinois Digital Environment for Access to Learning and Scholarship, March 15, 2019. https://doi.org/10.21900/iconf.2019.103373.

———. "Slipping through the Cracks: Background Investigations after Snowden." *Surveillance & Society* 15, no. 1 (2017): 123–36. https://doi.org/10.24908/ss.v15i1.5306.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California