

Literature on Personnel Vetting Processes and Procedures

Annotated Selected Bibliography

DAVID STEBBINS, SINA BEAGHLEY, ASHLEY L. RHOADES,
SUNNY D. BHATT

Prepared for the Performance Accountability Council Program
Management Office
Approved for public release; distribution unlimited



RAND NATIONAL DEFENSE RESEARCH INSTITUTE

For more information on this publication, visit www.rand.org/t/RR3172

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-0354-4

Published by the RAND Corporation, Santa Monica, Calif.

© Copyright 2019 RAND Corporation

RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Support RAND

Make a tax-deductible charitable contribution at
www.rand.org/giving/contribute

www.rand.org

Preface

The purpose of this work is to inform U.S. policymakers tasked with improving the Security, Suitability, and Credentialing (SSC) process and who are particularly focused on modernizing the vetting process. This annotated selected bibliography is organized around 13 categories of information intended to provide baseline policies, procedures, and literature, as well as offer new or emerging areas of insight related to potential personnel vetting improvements. This bibliography also references canonical judicial cases that have already affected or have the potential to affect future vetting policy considerations, particularly with regard to privacy concerns and other issues related to civil rights. Lastly, this bibliography offers insight into how the Five Eyes community partners (the United States, the United Kingdom, Australia, New Zealand, and Canada) conduct security vetting with respect to their current laws and policies, which could offer U.S. vetting practitioners points of comparison and insights regarding partnership efforts that might be considered in the U.S. modernization effort.

This research was sponsored by the Performance Accountability Council Program Management Office and conducted within the Cyber and Intelligence Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

For more information on the RAND Cyber and Intelligence Policy Center, see www.rand.org/nsrd/ndri/centers/intel or contact the center director (contact information is provided on the webpage).

Contents

Preface	iii
Summary	vii
Acknowledgments	xi
Abbreviations	xiii
 CHAPTER ONE	
Introduction	1
Project Background and Tasking	1
Methodology and Organization	2
Scope	3
 CHAPTER TWO	
Personnel Vetting Practices	5
Artificial Intelligence, Computational Tools, and Statistical Methods	6
Behavioral Detection	10
Social Media and Sentiment Analysis	15
Cybervetting	16
 CHAPTER THREE	
Preinvestigation and Investigation	19
Vetting for Employment	20
Privacy, Civil Liberties, and Legal Concerns	31
 CHAPTER FOUR	
Adjudication and Adjudication Bias	35
Adjudication Guidelines and Practices	36
Adjudication Bias	37
Adjudication Legal Concerns	38
 CHAPTER FIVE	
Suitability, Fitness, and Contractor Vetting	41
Suitability and Fitness Practices	42
Contractor Vetting	45

CHAPTER SIX

Insider Threats	47
Insider Threat Practices and Challenges	48
Detection and Prevention Mechanisms	50
Cloud-Based Insider Threats	57

CHAPTER SEVEN

Continuous Monitoring and Continuous Evaluation	59
--	----

CHAPTER EIGHT

Trust in the Workplace	65
Trust in the Workforce	66
Modeling Trust	67
Other Characteristics of Trust (Personalities and Building Trust)	68

CHAPTER NINE

Asset Protection	73
Places (Critical Infrastructure and Site Locations)	74
Physical Assets	76
Information and Intellectual Property	78

CHAPTER TEN

Organizational Resiliency and Risk Assessment	83
--	----

CHAPTER ELEVEN

Fraud Detection	87
------------------------------	----

CHAPTER TWELVE

Credentialing	93
----------------------------	----

CHAPTER THIRTEEN

Information Sharing and Reciprocity	99
--	----

CHAPTER FOURTEEN

Five Eyes Partner Practices	105
United Kingdom	105
Australia	109
New Zealand	112
Canada	115

APPENDIXES

A. Table of Bibliography Sources, by Category	117
B. U.S. Policy and Law Relevant for Categories	163
C. Boolean Search Terms and Strings	173
References	175

Summary

U.S. government vetting processes and procedures for public trust and national security positions are evolving to improve their effectiveness and to incorporate new technological capabilities. The rise of social media and other sources of information not historically used for vetting purposes are increasingly enhancing legacy vetting systems that otherwise might not uncover a prospective government employee's or contractor's propensity to cause harm to national security institutions. This reform effort is intended to protect government systems, information, and assets by ensuring aligned, effective, efficient, secure, and reciprocal processes to support a trusted federal workforce.

At the request of the Performance Accountability Council Program Management Office, RAND Corporation experts researched, reviewed, and assembled a selected bibliography of relevant literature related to government and other relevant vetting processes and procedures. This annotated selected bibliography provides a set of baseline literature in this area and offers new or emerging areas of insight related to potential personnel vetting improvements. The bibliography is organized into 13 categories, with each chapter containing a short summary and analysis of what the RAND team found within that chapter's respective literature. It presents what the team identified as the most-relevant available, open-source, or publicly available literature, recognizing that there may be additional relevant literature held at a classified or restricted level or otherwise unavailable to the general public.

The bibliography is divided into one category per chapter to help bin the literature and orient readers to understand different U.S. government vetting practice challenges and best practices, depending on the particular problem set to be addressed. The first chapter surveys relevant emerging global technologies that will affect future vetting practices. Commercial-off-the-shelf technology has become a significant factor in the way vetting is performed and will drive future U.S. government vetting requirements and tools.

Chapters Two through Five provide baseline and foundational information about personnel vetting and processes, including preinvestigation and investigation procedures, adjudication, and suitability and contractor vetting practices. This information was collected and assembled just prior (FY 2019) to the transfer of Security, Suitability, and Credentialing management responsibilities from the National Background Investi-

gations Bureau to the U.S. Department of Defense. Chapter Two provides selected literature focused on foundational aspects of modern personnel vetting, including examining artificial intelligence, methods for modeling risk, modes of behavioral detection, social media and sentiment analysis, and vetting practices in the cyber realm. Next, because the preliminary stages of the U.S. government vetting process play an important role in safeguarding U.S. national security, Chapter Three provides selected literature that documents the initial stage (preinvestigation) and subsequent investigation stage of the U.S. government vetting process, including sector-specific best practices. Adjudication decisions also serve as an important final vetting function within the Security, Suitability, and Credentialing process. Chapter Four presents selected literature on federal department and agency adjudication guidelines and practice and also includes information on how to identify and address adjudication bias. This chapter also contains important legal decisions related to current and future adjudication practices. Lastly, Chapter Five, on suitability, presents extensive material related to determining suitability and fitness eligibility. Information related to contractor vetting is sparse, however, which offers security managers no established baseline to create effective procedures.

Chapters Six and Seven provide an overview and literature related to two related U.S. government practices that pertain to individuals already adjudicated into sensitive positions: insider threats and continuous monitoring and continuous evaluation, respectively. Understanding, preventing, and mitigating the effects of insider attacks represented major themes throughout the literature examined in Chapter Six. Although actual definitions of *insider threats* are varied and largely dependent on the sector examined, the literature provided useful groupings that we present to assist in developing target insider threat programs. Two closely associated vetting mechanisms (continuous evaluation and continuous monitoring) and associated data collection are then examined in Chapter Seven, focusing on current U.S. government and private-sector practices. Here, the literature indicates that the implementation of both programs has been met with mixed success.

Chapters Eight and Nine focus on trust in the workplace and asset protection, respectively, and are closely aligned with the U.S. government's new Trusted Workforce 2.0 initiative. Chapter Eight identifies various personality traits, through the use of selected longitudinal and case study research designs, that can provide Trusted Workforce 2.0 managers with a substantive understanding of current research findings and impediments. Much of the literature in this chapter suggests the prioritization of longitudinal research to develop distinct case studies on trust. Chapter Nine, on asset protection, defined in the context of places, physical assets, information, and intellectual property, presents literature on the nexus between personnel vetting and the protection of U.S. assets. Literature here suggests that there is not a commonly shared definition of *asset protection*. Several of the publications referenced in this chapter include cases that had a lack of robust oversight protection mechanisms, which

contributed to loss of government platforms, and other situations in which the use of foreign contractors revealed vulnerability in supply chains. Other literature suggests that the U.S. government may become overreliant on high-tech solutions; physical (human) observation remains critical.

Chapter Ten consists of literature related to organizational resilience, highlighting research that shows situations in which personnel vetting considerations could affect resiliency efforts across different sectors. Literature here shows that an organization's ability to sustain operations in light of internal and external shocks can mitigate various risks associated with national security.

Chapter Eleven focuses on fraud detection programs. Such programs, implemented in both the public and private sectors, have application to U.S. government vetting practices. Chapter Eleven draws from both the banking and gaming (casino) industries and reveals scenarios in which structuring continuous vetting programs may be useful. Chapter Twelve addresses the issue of credentialing, which is a substantial requirement of U.S. government vetting and relates to the different types of accesses an individual might gain once adjudicated. The credentialing information in Chapter Twelve provides information about baseline policies for various government credentialing programs and some of the related barriers organizations face when implementing credentialing policy.

Chapter Thirteen relates to information-sharing and reciprocity agreements between federal departments and agencies. These are fundamental to the personal vetting process; however, U.S. government departments and agencies have struggled to implement security clearance reciprocity among the executive branch. Literature in Chapter Thirteen reveals that proper information exchange can relay important facts to an investigator regarding an individual's particular history and helps cross-validate information gained during interviews. Reciprocity functions become important once employees are adjudicated, especially when an individual might be negatively adjudicated for one agency yet can gain access to similar information through another agency.

Finally, Chapter Fourteen addresses practices, policies, and procedures of the United States' Five Eyes (FVEY) community partners (the United Kingdom, Australia, New Zealand, and Canada). This chapter provides selected literature regarding how U.S. FVEY partners conduct vetting, noting unique practices that may be relevant for U.S. policymakers to consider.

Acknowledgments

Our RAND team owes its gratitude to many individuals and organizations for making this selected annotated bibliography possible. We would like to thank the U.S. government vetting officials who provided helpful insights for the project. Our sponsors at the Performance Accountability Council Program Management Office provided excellent support, guidance, and feedback to the team throughout the creation of this bibliography, and we are grateful to them for this assistance. We would also like to thank Larry Hanauer and Charles Sowell, who served as peer reviewers and improved the final product as a result of their feedback. Numerous RAND experts and colleagues are deserving of our gratitude for valuable reviews and feedback, particularly Phillip Carter and Douglas Ligor, who provided deep knowledge of applicable U.S. security clearance and vetting case law. Lastly, our team would like to thank Betsy Hammes, an employee with RAND's Knowledge Services staff whose ability to deliver quality sources greatly affected the work herein.

Abbreviations

AGSVA	Australian Government Security Vetting Agency
AI	artificial intelligence
C.F.R.	Code of Federal Regulations
CSIS	Canadian Security Intelligence Service
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
FBI	Federal Bureau of Investigation
fMRI	functional magnetic resonance imaging
FVEY	Five Eyes
FY	fiscal year
GAO	U.S. Government Accountability Office
IC	intelligence community
IRS	Internal Revenue Service
ISAC	Information Sharing and Analysis Center
IT	information technology
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NBIB	National Background Investigations Bureau
NISP	National Industrial Security Program
NZSIS	New Zealand Security Intelligence Service

ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PAC	Performance Accountability Council
PERSEREC	Defense Personnel and Security Research Center
PMO	Program Management Office
PSR	Protective Security Requirements
RADAR	Review of Adjudication Documentation Accuracy and Rationales
SSC	Security, Suitability, and Credentialing
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
UKSV	United Kingdom Security Vetting
U.S.C.	U.S. Code
VA	U.S. Department of Veterans Affairs

Introduction

Project Background and Tasking

U.S. government vetting processes and procedures for public trust and national security positions are evolving to improve their effectiveness and to incorporate new technological capabilities. The rise of social media and other sources of information not historically used for vetting purposes are increasingly enhancing legacy vetting systems that otherwise might not uncover a prospective government employee or contractor propensity to cause harm to national security institutions. This reform effort is intended to protect government systems, information, and assets by ensuring aligned, effective, efficient, secure, and reciprocal processes to support a trusted federal workforce.

The role of the Performance Accountability Council (PAC) Program Management Office (PMO) in this space is, in part, to improve the Security, Suitability, and Credentialing (SSC) line of effort and implement personnel vetting reform across the U.S. government and in support of the Trusted Workforce 2.0 effort. The Office for the Director of National Intelligence (ODNI) announced the Trusted Workforce 2.0 initiative in March 2018 as a means to “identify and establish a new set of policy standards that will transform the U.S. government’s approach to vetting its workforce, overhaul the enterprise business processes, and modernize information technology.”¹ The main drivers behind the vetting reform are the national security and suitability investigation backlog, the quality of investigations conducted, the costs associated with vetting practices, and the continued integrity of government employees with access to sensitive and classified information.

In support of this line of effort, PAC PMO asked the RAND Corporation to develop an annotated bibliography that identifies key sources of personnel vetting procedures that could be used as a basis for considering new vetting methods and procedures for the U.S. government. The resultant annotated selected bibliography addresses current U.S. government practices, policies, and procedures, as well as those of the

¹ Brian Dunbar, “Statement for the Record for Brian Dunbar, Assistant Director, Special Security Directorate, National Counterintelligence and Security Center,” testimony before the Senate Select Committee on Intelligence Hearing on Security Clearance Reform, March 7, 2018.

United States' Five Eyes (FVEY) community partners (the United Kingdom, Australia, New Zealand, and Canada), and it also highlights research conducted within the private sector and academic institutions.

Methodology and Organization

The research team identified and extracted sources via RAND's access to EBSCOHost, ProQuest, LexisNexis, and Nexis Uni, which collectively returned approximately 300 results. From those, we selected and narrowed emerging literature and key practices across a variety of sources. In collaboration with PAC PMO, we coordinated a set of search terms of interest to PAC PMO and translated these into complex Boolean search strings to ensure targeted collection within the databases (see Appendix C for search terms and strings used). Although this method provided robust return of baseline literature, we found three specific literature gaps: information on adjudication bias, organizational resiliency, and fraud. To address the gaps, we performed additional, refined searches in the databases and online to mitigate the lack of database findings and noted remaining gaps, where merited.

The baseline literature collection was then vetted with RAND subject-matter experts who offered valuable insight and additional sources for consideration for this bibliography. In particular, we added sources of canonical judicial cases that have already affected—or have the potential to affect—vetting policy considerations, particularly with regard to privacy concerns and other civil rights–related issues. (Pertinent cases are listed under “Adjudication Legal Concerns” in Chapter Four.) We also held a collaborative feedback session with RAND colleagues to discuss project approach, categories, and findings. Finally, members of the team held an informal discussion with senior leadership within the FVEY community partners to identify country-specific information related to vetting practices to inform that area of research.

This selected annotated bibliography is organized into 13 categories, one per chapter, with each chapter containing a short summary and analysis of what our team found within that section's respective literature. The categories are as follows: personnel vetting practices; preinvestigation and investigation; adjudication and adjudication bias; suitability, fitness, and contractor vetting; insider threats; continuous monitoring and continuous evaluation; trust in the workplace; asset protection; organizational resiliency and risk assessment; fraud detection; credentialing; information sharing and reciprocity; and FVEY partner practices. Following the main body of this document, there are three appendixes. Appendix A provides a table of the literature contained in the selected annotated bibliography by associated category and includes URLs, where available, for quick reference; the table also indicates whether the hyperlink requires a subscription fee to access the document. Appendix B provides a table of relevant U.S. government policies, orders, laws, and guidance that pertain to categories in this anno-

tated bibliography. Appendix C provides a description of the Boolean search terms and strings used in this research.

Scope

This annotated selected bibliography contains a compilation and review of literature related to categories of information and search terms that were developed in conjunction with PAC PMO. It presents selected literature for identified categories, where applicable (e.g., vetting practices, insider threats, asset protection, organizational resilience, credentialing), each prefaced with a brief summary and analysis of findings. At the request of PAC PMO, the majority of the focus of this annotated bibliography is on analysis of personnel vetting and SSC governmental processes. However, in some chapters, we do highlight key or foundational governmental baseline policies, guidelines, and literature; then, in Appendix B, we provide a more detailed list of relevant U.S. government policies, orders, laws, and guidance.

The resulting annotated bibliography represents what the research team identified as the most-relevant literature and articles, in part, based on their relevance to personnel vetting and informed by PAC PMO guidance and prioritization. It highlights key practices and potential innovative approaches, where applicable, from the public and private sectors and academic institutions. The annotated bibliography also includes URLs to the publications, where available. This annotated bibliography is not intended to be an exhaustive list of every article and piece of literature that might pertain to personnel vetting but instead is intended to provide a selection of literature that the RAND team identified as the most relevant publicly available and unclassified sources, based in part on our own informed judgment and on PAC PMO guidance and prioritization. This document is not inclusive of relevant literature at the classified or restricted level or material that is otherwise publicly unavailable.

Personnel Vetting Practices

Emerging global technologies are driving how future vetting practices are conducted and will need to be carefully monitored for applicability to vetting. Whereas technology developed by the military and other U.S. government entities drove innovation in commercial technology (e.g., GPS, drones, synthetic materials), this paradigm now is shifting to private-sector innovation, which is driving government application. Advances in artificial intelligence (AI), behavioral detection, social media, cloud computing architectures, and other methods to model risk to such systems arrive in the form of academic and commercial pursuits and can serve as force multipliers for the vetting of future government employees.

In April 2019, the President issued Executive Order 13869, which transferred responsibility for background investigations from the National Background Investigations Bureau (NBIB) to the U.S. Department of Defense (DoD). DoD's Defense Counterintelligence and Security Agency now serves as the primary component for the National Industrial Security Program (NISP) and executes responsibilities relating to "continuous vetting, insider threat programs, and any other responsibilities assigned to it by the Secretary of Defense consistent with law."¹ This transfer is in its very early stages, but one of the key challenges will be ensuring that personnel from other agencies are investigated and cleared in the same timely manner, notwithstanding the fact that DoD personnel and contractors represent about 90 percent of the cleared population.²

¹ Executive Order 13869, *Transferring Responsibility for Background Investigations to the Department of Defense*, Washington, D.C.: White House, April 24, 2019.

² We received feedback from a former U.S. government employee and security clearance subject-matter expert who indicated that "smaller agencies, like the Departments of State, Treasury, Energy, and Homeland Security, are understandably concerned that their personnel will become a lesser priority—particularly since DoD personnel and contractors represent roughly 90 percent of people with clearances." This feedback also suggested that there may be lessons to be learned from the private sector on how to ensure that "secondary" customers—such as those without influence over decisionmaking processes or significant impact on revenues—can be served effectively.

In February 2019, the President issued Executive Order 13859, *Maintaining American Leadership in Artificial Intelligence*,³ the first on the topic, as DoD simultaneously unveiled its vision for incorporating AI into a number of programs within the department, with the intention of institutionalizing machine learning programs throughout the U.S. government and drawing heavily on close cooperation among the public sector, the private sector, and academia.⁴

This section includes selected literature examining AI, methods for modeling risk, modes of behavioral detection, social media and sentiment analysis, and vetting practices in the cyber realm. The selected annotations draw important connections on the way personnel vetting is currently conducted and possible approaches for future implementation.

Artificial Intelligence, Computational Tools, and Statistical Methods

Ahmad, Maaz Bin, Adeel Akram, M. Asif, and Saeed Ur-Rehman, "Using Genetic Algorithm to Minimize False Alarms in Insider Threats Detection of Information Misuse in Windows Environment," *Mathematical Problems in Engineering*, 2014.
<https://www.hindawi.com/journals/mpe/2014/179109/abs/>

This article from a group of researchers in Pakistan provides methods for categorizing user behavior within information environments. Researchers find that classifying behavior patterns at the onset of any monitoring program will reduce the incidence of false positives associated with user activity.

Allen, Greg, and Taniel Chan, *Artificial Intelligence and National Security*, Cambridge, Mass.: Belfer Center for Science and International Affairs, 2017.
<https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf>

This report presented by the Harvard Kennedy School's Belfer Center proposes a set of three goals to develop U.S. policy for AI within national security. The first part discusses how best to preserve "U.S. technological leadership," through "supporting peaceful and commercial" AI use, and provides various suggestions on how federal departments and agencies can attempt to mitigate associated risks. The report then delves into four cases that focus on transformative military technology—nuclear, aerospace, cyber, and biotech—before offering a part on lessons learned and, finally, policy recommendations for U.S. leadership.

³ Executive Order 13859, *Maintaining American Leadership in Artificial Intelligence*, Washington, D.C.: White House, February 11, 2019.

⁴ Terri Moon Cronk, "DoD Unveils Its Artificial Intelligence Strategy," U.S. Department of Defense, February 12, 2019.

Alpaydin, Ethem, *Machine Learning: The New AI*, Cambridge, Mass.: MIT Press, 2016.

http://www.harvard.com/book/machine_learning_the_new_ai_the_mit_press_essential_knowledge_series/

This book focuses on the theories of machine learning and serves as foundational reading for how to understand turning “data into knowledge.” The author traces how digital technology has transformed from “number-crunching mainframes to mobile devices,” putting “today’s machine learning boom in context.” The book also notes future implications for AI and machine learning, noting some ethical and legal considerations for future data privacy and security.

Bailey, Kyle O., James S. Okolika, and Gilbert L. Peterson, “User Identification and Authentication Using Multi-Modal Behavioral Biometrics,” *Computers and Security*, Vol. 43, 2014, pp. 77–89.

<https://www.sciencedirect.com/science/article/pii/S0167404814000340>

This article suggests a method to prevent malicious computer attacks through the use of a behavioral biometric system that creates a computer profile based on keystroke data, mouse movement, and user interface windows. The authors suggest that the combination of methods can reveal a more accurate depiction of system use rather than relying on a single method of detection, and they develop case studies to support findings of increased false acceptance rates.

Congressional Research Service, *Artificial Intelligence and National Security*, Washington, D.C., January 30, 2019.

<https://fas.org/sgp/crs/natsec/R45178.pdf>

The U.S. Congress has key interests in understanding AI impacts and has tasked the Congressional Research Service to analyze the ways it can assist government operations. This publication provides a comprehensive overview of U.S. government use of AI. It seeks to answer such questions as the following: (1) What is the right balance of commercial and government funding for AI development? (2) How might Congress influence defense acquisition reform initiatives that facilitate military AI development? (3) What changes, if any, are necessary in Congress and DoD to implement effective oversight of AI development? (4) How should the United States balance research and development related to AI and autonomous systems with ethical considerations? (5) What legislative or regulatory changes are necessary for the integration of military AI applications? (6) What measures can Congress take to help manage the AI competition globally? The publication also surveys current use of AI within the realm of military and intelligence operations and provides insight into the future use of AI for such implications.

Greitzer, Frank, L., and Ryan E. Hohimer, "Modeling Human Behavior to Anticipate Insider Attacks," *Journal of Strategic Security*, Vol. 4, No. 2, 2011.

<https://scholarcommons.usf.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1094&context=jss>

Researchers describe a predictive modeling framework for insider threat analysis that integrates a diverse set of data sources from the cyber domain, as well as infer psychological or motivational factors that might underlie malicious insider exploits. This comprehensive threat assessment approach provides automated support for the detection of high-risk behavioral "triggers" to help focus the analyst's attention and inform the analysis.

Grover, Justin, "Android Forensics: Automated Data Collection and Reporting from a Mobile Device," *Digital Investigation*, Vol. 10, Suppl., 2013.

<https://www.sciencedirect.com/science/article/pii/S1742287613000480>

In this research, a prototype enterprise monitoring system for Android smartphones was developed to continuously collect many data sets of interest to incident responders, security auditors, proactive security monitors, and forensic investigators. An anti-forensics analysis on the system was performed to identify and further strengthen areas vulnerable to tampering. The contributions of this research include the release of the first open-source Android enterprise monitoring solution of its kind, a comprehensive guide of data sets available for collection without elevated privileges, and the introduction of a novel design strategy implementing various Android application components useful for monitoring on the Android platform.

Kandias, Miltiadis, Dimitris Gritzalis, Vasilis Stavrou, and Kostas Nikoloulis, "Stress Level Detection via OSN Usage Pattern and Chronicity Analysis: An OSINT Threat Intelligence Module," *Computers and Security*, Vol. 69, 2017, pp. 3–17.

<https://www.sciencedirect.com/science/article/pii/S0167404816301742>

This article analyzes data collected via open-source intelligence in online social networks to test the stress levels users experienced. The researchers argue that the monitoring of user stress levels can help with insider threat detection, as stress is one proven indicator of the level of risk posed by an individual.

Mathis, Christi, "SIU Helps Create the World's First Centralized System for Evaluating Degrees, Licenses and Other Professional Credentials," Southern Illinois University, December 11, 2017.

<https://news.siu.edu/2017/12/>

[121117-centralized-professional-credential-system.php](https://news.siu.edu/2017/12/121117-centralized-professional-credential-system.php)

This news release discusses the creation of Credential Registry, a cloud-based repository and service for credentialing information, consisting of degrees, certificates, licenses, badges, apprenticeships, industry certifications, microcredentials, and similar earned recognitions. Students can use the registry to see which credentials are needed for vari-

ous career pathways and easily compare the credentialing options based on key data points, such as competencies and cost, while employers can use the registry to glean critical competency information from job applicants to determine who would best fulfill their workforce needs.

Mills, Jennifer U., Jason R. Dever, and Steven M. F. Stuban, "Using Regression to Predict Potential Insider Threats," *Defense Acquisition Research Journal*, Vol. 25, No. 2, 2018, pp. 122–157.

<https://www.dau.mil/library/arj/p/ARJ-85>

This research reviews potential insider threats against ship systems and simulates possible insider threat scenarios using system and device access data from both normal and malicious users. A regression-based model is used to validate the hypothesis that normal user behaviors are substantially different from malicious user behaviors. By observing and identifying different characteristics and unusual behaviors, the research concludes that recognizing and monitoring emerging patterns can help identify potential insider threats.

Punithavathani, D. Shalini, K. Sujatha, and J. Mark Jain, "Surveillance of Anomaly and Misuse in Critical Networks to Counter Insider Threats Using Computational Intelligence," *Cluster Computing*, Vol. 18, No. 1, 2015, pp. 435–451.

<https://link.springer.com/article/10.1007/s10586-014-0403-y>

This article suggests a method for surveilling insider threats across two phases of operations: The first phase involves capturing information packets sent via computer networks in transit, while the second phase involves analyzing the informational elements (log files) incoming and outgoing packets to develop information-use patterns. The article finds that this two-step model can help assess whether a user's activity deviates from the baseline assessment, called the Dempster-Shafer theory.

Al Tabash, Kholood, and Jassim Happa, "Insider-Threat Detection Using Gaussian Mixture Models and Sensitivity Profiles," *Computers and Security*, Vol. 77, 2018.

<https://www.sciencedirect.com/science/article/pii/S0167404818302487>

A challenge for insider threat detection is creating a behavioral threat detection system that does not produce a great number of false positives. An approach is put forward that combines automated anomaly detection and the knowledge of security analysts to lower the number of false positives. The solution requires the following functionalities: (1) the ability to compute a vector representation of employees' activities, (2) the ability for automated anomaly detection, (3) the ability to communicate information to security analysts for analysis of detected anomalies, (4) the ability to provide analysts with the capability of classifying detected anomalies, and (5) the ability to include nontechnical indicators of insider threat as part of the detection system.

Twyman, Nathan W., Paul Benjamin Lowry, Judee K. Burgoon, and Jay F. Nunamaker Jr., "Autonomous Scientifically Controlled Screening Systems for Detecting Information Purposely Concealed by Individuals," *Journal of Management Information Systems*, Vol. 31, No. 3, 2014, pp. 106–137.
<https://www.tandfonline.com/doi/abs/10.1080/07421222.2014.995535>

This study from the *Journal of Management Information Systems* suggests the use of an emerging technology called Autonomous Scientifically Controlled Screening Systems (ASCSS), which can aid in the detection of individuals' "purposely hidden information about target topics of interest." For example, such hidden topics can include "knowledge of concealed weapons, privacy violations, fraudulent organizational behavior, organizational security policy violations, preemployment behavioral intentions, organizational insider threat, leakage of classified information, and consumer product use information." The authors believe that ASCSS offers a technical methodology that can help represent a "systematic synthesis of structured interviewing, orienting theory, defensive response theory, noninvasive psychophysiological measurement, and behavioral measurement."

Behavioral Detection

Brickfield, Francis X., "Improving Scrutiny of Applicants for Top Secret/SCI Clearances by Adding Psychological Assessments," *National Security Law Journal*, Vol. 2, No. 2, 2013.
https://www.nslj.org/wp-content/uploads/2_NatlSecLJ_252-300_Brickfield.pdf

This article offers research on how the use of psychological screening, in addition to other legacy background checks, can improve applicant vetting processes. The author uses the case of psychological screening for prospective law enforcement personnel to suggest additional applicability to normal Security, Suitability, and Credentialing (SSC) processes. The article also notes some important legal and policy considerations in applying psychological screening, discussing U.S. Supreme Court rulings in the *Department of the Navy v. Egan* and *NASA v. Nelson*.

Colomb, Cindy, Magali Ginet, Daniel Wright, Samuel Demarchi, and Christophe Sadler, "Back to the Real: Efficacy and Perception of a Modified Cognitive Interview in the Field," *Applied Cognitive Psychology*, Vol. 27, No. 5, September/October 2013.
<https://doi.org/10.1002/acp.2942>

This journal article surveys developments in the field of cognitive science in relation to cognitive interviewing techniques. The authors state that, although many experiments regarding cognitive interviewing have been published, very few have tested its validity in real-world settings. The authors address this gap by conducting a modified cognitive interview (MCI) test in a law enforcement context, finding that the MCI produced the

most “forensically relevant” information, especially when conducted on the victims of crime.

Elifoglu, I. Hilmi, Ivan Abel, and Ozlem Tasseven, “Minimizing Insider Threat Risk with Behavioral Monitoring,” *Review of Business*, Vol. 38, No. 2, 2018, pp. 61–74.
<https://www.ignited.global/case/business/minimizing-insider-threat-risk-behavioral-monitoring>

The authors of this article suggest that enhanced behavioral monitoring can help minimize the insider threat by exposing indicators or red flags regarding an individual’s behavior. The article suggests that increased collaboration and information exchange between the informational technology management and human resources departments in companies would result in an improved ability for organizations to predict and detect risky behavior and potential insider threats.

Greitzer, Frank L., Lars J. Kangas, Christine F. Noonan, Christopher R. Brown, and Thomas Ferryman, “Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis,” *e-Service Journal: A Journal of Electronic Services in the Public and Private Sectors*, Vol. 9, No. 1, 2013, pp. 106–138.
<https://www.jstor.org/stable/10.2979/eservicej.9.1.106>

This journal article investigates various cases of insider abuse to provide further research on how different types of behaviors correlate with the potential to abuse information systems. Researchers use personality-trait modeling and develop a word taxonomy based on personality indicators. This model is then applied to a sample email population to validate findings.

Hills, Mils, and Anjali Anjali, “A Human Factors Contribution to Countering Insider Threats: Practical Prospects from a Novel Approach to Warning and Avoiding,” *Security Journal*, Vol. 30, No. 1, 2017, pp. 142–152.
<https://link.springer.com/article/10.1057/sj.2015.36>

This article gives an overview of the insider threat concept and problem and offers ways to detect and combat the insider threat. This includes a discussion of technical measures, consisting of procedures, controls, and policies, and the shortcomings of such methods. There is also discussion of information systems that sense changes in the environment and in the behavior of users. The authors emphasize that management and operational leaders must work together to build on best practices across industries.

Ho, Shuyuan Mary, Michelle Kaarst-Brown, and Izak Benbasat, “Trustworthiness Attribution: Inquiry into Insider Threat Detection,” *Journal of the Association for Information Science and Technology*, Vol. 69, No. 2, 2018, pp. 271–280.
<https://onlinelibrary.wiley.com/doi/pdf/10.1002/asi.23938>

This article offers a theoretical lens for analyzing existing research and literature on insider threat detection. The authors argue that changes in communication patterns

within a group, particularly computer- or online-based interactions, can reflect shifts in trustworthiness surrounding individuals who have breached a community's trust and thereby serve as an indicator that an individual may be a traitor or a threat. The article also highlights the importance of safeguarding proprietary, classified, or otherwise sensitive information in the cyber realm.

Jaros, Stephanie L., *A Strategic Plan to Leverage the Social and Behavioral Sciences to Counter the Insider Threat*, Monterey, Calif.: Defense Personnel and Security Research Center, TR-18-16, 2018.

<https://apps.dtic.mil/dtic/tr/fulltext/u2/1063771.pdf>

This report presents a strategic plan that the Office of the Under Secretary of Defense for Intelligence and the Defense Personnel and Security Research Center (PERSEREC) formulated to leverage the social and behavioral sciences to counter the insider threat within DoD. The plan hinges on five social and behavioral sciences research campaigns: employee reporting; technology, tools, and data; individual factors; organizational factors; and program evaluation. The overall goal of the plan is to integrate social and behavioral sciences research and tools into the DoD counter-insider threat mission and to ensure sustained investment in future social and behavioral sciences research.

Jaros, Stephanie L., Donna L. Tadle, David Ciani, Keith B. Senholzi, and Rene Dickerhoof, *Improving Mental Health Reporting Practices in Between Personnel Security Investigations*, Monterey, Calif.: Defense Personnel and Security Research Center, TR-17-07, 2017.

https://www.dhra.mil/Portals/52/Documents/perserrec/reports/TR-17-07_Improving_Mental_Health_Reporting_Practices.pdf

This report presents the results of a study evaluating trends in mental health reporting in the Joint Personnel Adjudication System, as well as related policies. The findings of the study suggest that the majority of reported incidents were tied to depression, suicidal thoughts, or suicide attempts and that policy should include clearer guidance on reporting requirements and procedures for helping subjects that express tendencies toward self-harm. The report also provides recommendations on how best to disseminate, monitor, and store mental health-related information across the personnel security community.

Kühn, Stephan, and Annamart Nieman, "Can Security Vetting Be Extended to Include the Detection of Financial Misconduct?" *African Security Review*, Vol. 26, No. 4, 2017, pp. 413–433.

<https://www.tandfonline.com/doi/pdf/10.1080/10246029.2017.1294096>

A national department within the government of South Africa found 19 individuals guilty of financial fraud, and the existing vetting processes failed to detect this conduct. Interviews with the department and subject-matter experts found that security

vetting can indeed be extended to include the detection of financial misconduct within the researched department. Also, it can enhance the management of fraud risk across all South African public-sector departments.

Morgan, Charles A., Yaron G. Rabinowitz, Deborah Hilts, Craig E. Weller, and Vladimir Coric, "Efficacy of Modified Cognitive Interviewing, Compared to Human Judgments in Detecting Deception Related to Bio-Threat Activities," *Journal of Strategic Security*, Vol. 6, No. 3, 2013, pp. 100–119.

<https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1249&context=jss>

This article speaks to the lack of empirical research needed to support various methods of detecting when individuals vying for a national security clearance engage in deceptive activities. The article suggests that applications from alternative interview methods, such as modified cognitive interviewing, have much higher rates for detecting deception during interviews. Modified cognitive interviewing has the advantage of removing human judgment, which the authors state is only about 50 percent effective. The authors develop a research environment employing a variety of interview techniques, with the goal of pinpointing deception during interviews, finding that modified cognitive interviewing could accurately detect deception in 84.4 percent of the situations examined.

Orthey, Robin, Aldert Vrij, Sharon Leal, and Hartmut Blank, "Strategy and Misdirection in Forced Choice Memory Performance Testing in Deception Detection," *Applied Cognitive Psychology*, Vol. 31, No. 2, March/April 2017.

<https://onlinelibrary.wiley.com/doi/full/10.1002/acp.3310>

This article applies a "cognitive hierarchy theory" (a model rooted in economic and game theory) in an attempt to trace human choice during a mock criminal act. The test involved several participants to better understand what specific strategies might be used to improve lie detection and specific cues to misdirect investigators. Researchers found eight types of strategies commonly used to "appear innocent" during testing and report mechanisms to detect different types of deception strategies.

Rogers, Richard, Adriel Boals, and Eric Y. Drogin, "Applying Cognitive Models of Deception to National Security Investigations: Considerations of Psychological Research, Law, and Ethical Practice," *Journal of Psychiatry and Law*, Vol. 39, No. 2, 2011, pp. 339–364.

https://heinonline.org/HOL/Page?handle=hein.journals/jpsych39&div=21&g_sent=1&casa_token=

This publication from the *Journal of Psychiatry and Law* lays out the legal and ethical considerations of using psychology to develop deception-detection mechanisms. The authors provide evidence of success using psychological based interviews and other investigative techniques to reduce possible legal and ethical violations for program managers.

Shedler, Jonathan, and Eric L. Lang, *A Relevant Risk Approach to Mental Health Inquiries in Question 21 of the Questionnaire for National Security Positions (SF-86)*, Monterey, Calif.: Defense Personnel and Security Research Center, TR-15-01, March 2015.

https://www.dhra.mil/Portals/52/Documents/perserrec/TR_15-01_A_Relevant_Risk_Approach_to_Mental_Health_Inquiries_in_Question_21.pdf

This report argues that the current approach to mental health inquiries—as provided for in question 21 of the SF-86, the National Security Questionnaire—is overly broad and flags too many individuals as potential risks in need of further investigation. To solve this issue, the authors propose a “relevant risk” approach based on more-quantifiable, standardized metrics for mental health conditions and hospitalizations. The authors suggest that this alternate approach would more accurately pinpoint individuals whose mental health conditions could pose actual security risks and would eliminate the need for superfluous investigations (and the associated expenses).

Vrij, Aldert, Samantha Mann, Susanne Kristen, and Ronald P. Fisher, “Cues to Deception and Ability to Detect Lies as a Function of Police Interview Styles,” *Law and Human Behavior*, Vol. 31, No. 5, October 2007, pp. 499–518.

https://www.jstor.org/stable/4499551?seq=1#metadata_info_tab_contents

This article examines different types of interviewing techniques, including criteria-based content analysis and reality monitoring to see whether there are certain “verbal cues” that can aid in the detection of deceit. The authors suggest that accusatory-style interrogations often provide short responses from suspects, providing limited insight into whether deception is being used. The authors find that the reality-monitoring method elicited more verbal responses that could be coded and offer additional insight into the suspect responses provided.

Vrij, Aldert, Christian A. Meissner, Ronald P. Fisher, Saul M. Kassin, Charles A. Morgan III, and Steven M. Kleinman, “Psychological Perspectives on Interrogation,” *Perspectives on Psychological Science*, Vol. 12, No. 6, 2017, pp. 927–955.

<https://journals.sagepub.com/doi/pdf/10.1177/1745691617706515>

The authors draw from psychological and other academic theory to support arguments against enhanced interrogation techniques. They find that (1) individuals will decrease rather than increase cooperation with interrogators, (2) adversarial techniques alter brain chemicals to inhibit memory recall, and (3) these techniques can detract from accurately detecting deception. Conversely, rapport-building measures are found to be much more effective at providing analyzable speech content, which, in turn, can assist with credibility assessment.

Social Media and Sentiment Analysis

Costello, A., and C. Potter, “#EpicFail: How to Avoid Social Media Disasters in the Hiring Process,” *Business Affairs*, Vol. 81, No. 4, 2015.

<http://www.mondaq.com/unitedstates/x/415174/employee+rights+labour+relations/EpicFail+How+To+Avoid+Social+Media+Disasters+In+The+Hiring+Process>

The use of social media is prevalent throughout all age groups in society, and employers are now using this information to evaluate an applicant during the hiring process. Although Americans are protected from unreasonable searches and seizures, information posted on social media is generally not private and is instantly distributed throughout the world. Some states have enacted legislation barring employers from gaining access to restricted information posted on social media. Others point out that, while investigating applicants’ social media accounts, employers could gain access to information that cannot be used in the hiring decision, such as race and nationality.

Security Executive Agent Directive 5, *Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications*, Version 5.4, Washington, D.C.: Office of the Director of National Intelligence, May 5, 2016.

<https://www.dni.gov/files/documents/Newsroom/Press%20Releases/SEAD5-12May2016.pdf>

This security executive agent directive establishes guidance for collecting and using social media data to inform personnel security background investigations and adjudication. This directive applies for “determining initial or continued eligibility for access to classified national security information or eligibility to hold a sensitive position and the retention of such information.”

Shaw, Eric, Maria Payri, Michael Cohn, and Ilene R. Shaw, “How Often Is Employee Anger an Insider Risk? Detecting and Measuring Negative Sentiment Versus Insider Risk in Digital Communications,” *Journal of Digital Forensics, Security and Law*, Vol. 8, No. 1, 2013.

<https://commons.erau.edu/jdfsl/vol8/iss2/3/>

This research uses a combination of rating scales to quantify negative-sentiment measurements as a method to test newly developed psycholinguistic software application (WarmTouch) to indicate potential insider threat risk. Although the software application tested poorly in identifying low levels of negative sentiment, the researchers do not believe that its use would inhibit overall usefulness for insider threat programs, given the program’s ability to locate true positives in sample populations.

Tayouri, David, "The Human Factor in the Social Media Security—Combining Education and Technology to Reduce Social Engineering Risks and Damages," *Procedia Manufacturing*, Vol. 3, 2015, pp. 1096–1100.

<https://www.sciencedirect.com/science/article/pii/S2351978915001821>

This article discusses the various risks to cybersecurity posed by social media use. The authors argue that social media "training" should begin in elementary school (first grade), since formal organizational policies have had minimal effect on workplace populations. The authors believe that instituting training programs early and often would help to strengthen "human factor" understanding of associated risks and methods of prevention.

Cybervetting

Berkelaar, Brenda L., and Patrice M. Buzzanell, "Cybervetting, Person–Environment Fit, and Personnel Selection: Employers' Surveillance and Sensemaking of Job Applicants' Online Information," *Journal of Applied Communication Research*, Vol. 42, No. 4, 2014, pp. 456–476.

<https://www.tandfonline.com/doi/full/10.1080/00909882.2014.954595>

This qualitative research examines how organizations combine cybervetting practices with predetermined organizational "fit" assessments. The research finds that many organizations develop fit assessments to maintain branding (reputation) and operational efficiency and to manage overall risk. Finally, this research recommends that, to best understand cybervetting's relationship to organizational fit, more assessment will be needed to link the actual effectiveness of the cybervetting to overall organizational outcomes.⁵

Ghoshray, Saby, "The Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-Vetting and Law's Inability to Catch Up," *John Marshall Review of Intellectual Property Law*, Vol. 12, 2013, pp. 551–582.

https://heinonline.org/HOL/Page?handle=hein.journals/johnmars12&div=23&g_sent=1&casa_token=&collection=journals

This article reviews relevant legal implications that organizations should consider as cybervetting practices continue to bolster more-traditional hiring mechanisms. The article notes that a lack of clear organizational policy for cybervetting potential employees across sectors, coupled with an "absence of robust laws" governing the use such practices, has complicated reasonable expectations of employee privacy over the past few years. The article concludes with several suggestions for how future employment law might be addressed to accommodate cybervetting while adhering to privacy

⁵ Also see Brenda L. Berkelaar, *Cyber-Vetting: Exploring the Implications of Online Information for Career Capital and Human Capital Decisions*, dissertation, West Lafayette, Ind.: Purdue University, 2010.

laws. In addition, the article finds that information gained from cybervetting should never be “conflated” with actual workplace behaviors.

King, Zoe M., Diane S. Henshel, Liberty Flora, Mariana G. Cains, Blaine Hoffman, and Char Sample, “Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment,” *Frontiers in Psychology*, Vol. 9, 2018.

<https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00039/full>

This article argues that the process of characterizing cybersecurity system risk must include human factors to better predict system vulnerability. The authors contend that rationality, expertise, and maliciousness are the three key human factors to consider when developing a cybersecurity risk plan. This article covers actions taken by the Cybersecurity Collaborative Research Alliance to develop the “Human Factors risk framework” toward identifying specific characteristics of attackers, users, and defenders to better mitigate the effects of a potential cyberattack.

Leggitt, John S., Olga G. Shechter, and Eric L. Lang, *Cyberculture and Personnel Security: Report I—Orientation, Concerns, and Needs*, Monterey, Calif.: Defense Personnel and Security Research Center, TR 11-01, May 2011.

<http://www.dhra.mil/Portals/52/Documents/perserec/tr11-01.pdf>

This first report (in a two-series volume) from PERSEREC examines the link between employee online behaviors and their possible impacts on workplace security. Research presented by PERSEREC intends to advance DoD policy, awareness, and personnel investigations and adjudication decisions. The report notes that all of the SSC investigation and adjudication standards were instituted before the proliferation of social media and other online methods of communication, though social media and online communications have become an important factor when weighing such national security decisions. PERSEREC notes that “online disinhibition[,] . . . where people who become more willing to disclose personal information, deceive, or become hostile, affects personnel security,” which has become a critical factor for further study.

Mikkelsen, Katherine, “Cybervetting and Monitoring Employees’ Online Activities: Assessing the Legal Risks for Employers,” *Public Lawyer*, Vol. 18, No. 2, 2010.

https://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2010/annualconference/161.pdf

This foundational legal article on the practice of cybervetting notes some of the policy implications associated with conducting open-source checks on prospective government employees. The author notes findings compiled in 2009 by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association, which found that 50 percent of government respondents lacked clear cybervetting policies, which presents numerous privacy concerns.

Paek, Tim, Michael Gamon, Scott Counts, David Maxwell Chickering, and Aman Dhesi, "Predicting the Importance of Newsfeed Posts and Social Network Friends," *Proceedings of the Twenty-Fourth AAAI Conference on Artificial Intelligence*, 2010. <http://maxchickering.com/publications/aaai10.pdf>

This study seeks to understand the strength of "friend" networks on social media platforms. The authors develop a classification system to bin the importance of newsfeeds, posts, and individual friends based on message text and historical interactions within such networks. The study was able to achieve an accuracy of 85 percent when trying to predict an individual's closest friends, offering some clear parallels for preemployment vetting.

Rose, Andrée, Howard Timm, Corrie Pogson, Jose Gonzalez, Edward Appel, and Nancy Kolb, *Developing a Cybervetting Strategy for Law Enforcement*, Monterey, Calif.: Defense Personnel and Security Research Center, December 2010. <http://www.iacpsocialmedia.org/wp-content/uploads/2017/02/CybervettingReport-2.pdf>

This foundational study from PERESERC defines *cybervetting* as the "assessment of a person's suitability to hold a position using information found on the Internet to help make that determination." This document also sets the stage for the ensuing legal discussions surrounding the use of cybervetting as a tool for preemployment checks, suggesting specific law-enforcement policies that should be established when considering past applicant behaviors and a social media-use framework for law enforcement officers on active duty.

Shechter, Olga G. Eric L. Lang, and Christina R. Keibler, *Cyber Culture and Personnel Security: Report II—Ethnographic Analysis of Second Life*, Monterey, Calif.: Defense Personnel and Security Research Center, TR-11-03, July 2011. <https://apps.dtic.mil/dtic/tr/fulltext/u2/a568713.pdf>

This report (the second in a two-series volume) from PERSEREC examines the link between employee online behaviors and possible impacts on workplace security, using the once-popular Second Life social media platform to develop a "typology for distinguishing between innocuous and problematic use of this cyber environment." The study involved interviews with 148 Second Life users who had the same demographical makeup as the security clearance population. The study finds that there were several reported behaviors that would constitute a review against adjudicative guidelines if indeed clearance holders exhibited the same behaviors in the virtual environment.

Preinvestigation and Investigation

The initial stages of the personnel vetting process serve an important gatekeeping function for the U.S. national security establishment. Even if there are effective monitoring systems in place once government employees or contractors gain access to sensitive information, having effective initial vetting processes can mean the difference between granting access to an established trusted individual or leaving the government open to a potential insider threat. Initial vetting processes (preinvestigation) also serve an important budgetary concern: Screening out individuals before they enter the investigation stage can save thousands of dollars in costs associated with the investigation stage.

This chapter includes selected literature related to these initial stages of preinvestigation and investigation of the U.S. vetting process for employment and includes literature from across sectors, such as literature examining vetting best practices.¹ This chapter concludes with a sampling of ethical and legal literature offering considerations for practitioners to inform future vetting program policies.² For example, literature from the U.S. Government Accountability Office (GAO) and DoD identifies new methods for detecting employee financial strain that many times will be omitted from vetting forms (SF-85 and SF-86). Other examples in the chapter reveal how the Transportation Security Administration (TSA) has modernized its vetting practices to screen both pilots and airport workers to improve airport security, the barriers that

¹ The vetting stage of adjudication is presented in Chapter Four, and reinvestigation is included in Chapter Thirteen, under continuous monitoring and continuous evaluation.

² There have been some constitutional concerns for U.S. practices in this area that have been challenged both at the Supreme Court level and within lower-level district courts. For example, *Griswold v. Connecticut* (1965) and *United States v. Maynard* both draw attention to privacy considerations. *Griswold v. Connecticut* was the first case to identify personal privacy as a constitutional right, while *United States v. Maynard* (2010) has served as the basis for obtaining warrants to monitor individual citizens. These two canonical court cases have served as modern precedent for cases pursuant to the USA PATRIOT ACT (Pub. L. 107-56) and other surveillance programs that affect how vetting practices are performed. For example, using open-source research (a form of cybervetting) can fill information gaps on whether an individual is suitable for government service, which is difficult to validate and can run afoul of the standards of conduct for social media under 5 C.F.R. 2635.

investigators face when requesting state-level criminal record information, and several other reports on the timeliness and effectiveness of initial security clearances stages.

Vetting for Employment

Aronow, Peter, Alexander Coppock, Forrest W. Crawford, and Donald P. Green, "Combining List Experiment and Direct Question Estimates of Sensitive Behavior Prevalence," *Journal of Survey Statistics and Methodology*, Vol. 3, No. 1, March 2015, pp. 43–66.

<https://academic.oup.com/jssam/article/3/1/43/915561>

This article explores possible relationships between direct questioning by investigators and truthful responses by individuals and suggests a study design for carrying this research forward. The authors find that individuals prefer to remain "socially attractive" when responding to direct questioning and many times answer in the way they expect their questioner wants to hear. Instead, the authors advocate for the use of a "list experiment," where respondents are provided a set list of items that, for example, asks how many of the items they may or may not agree with, rather than the direct approach, which would ask "which one don't you agree with."

Bagdoyan, Seto J., U.S. Government Accountability Office, "Additional Mechanisms May Aid Federal Tax-Debt Detection," testimony before the Subcommittee on Government Operations, Committee on Oversight and Government Reform, House of Representatives, March 18, 2015.

<https://www.gao.gov/assets/670/669073.pdf>

This testimony summarizes the findings of previous GAO reports on federal tax debts owed by DoD employees and contractors and provides recommendations from previous reports for how to improve the detection of federal tax debt in the vetting and security clearance process.

Booth-Kewley, Stephanie, Gerald E. Larson, David L. Alderton, William L. Farmer, and Robyn Highfill-McRoy, "Risk Factors for Misconduct in a Navy Sample," *Military Psychology*, Vol. 21, No. 2, 2009, pp. 252–269.

<https://www.tandfonline.com/doi/full/10.1080/08995600902768776>

This study observed a sample of Navy personnel to identify psychosocial risk factors for misconduct or antisocial behavior. Researchers compared two groups of sailors: one that had engaged in misconduct within the Navy and one that had not. The study identified alcohol use, high impulsivity, hostility, and antisocial behavior of the subjects' friends as the most important risk factors for antisocial behavior. A strong correlation between heavy drinking and misconduct and related disciplinary action emerged. The researchers asserted that these findings were consistent with the results of studies on other problem behaviors in adolescent and adult populations.

Bunn, Geoffrey C., *The Truth Machine: A Social History of the Lie Detector*, Baltimore, Md.: Johns Hopkins University Press, 2012.
<https://jhupbooks.press.jhu.edu/title/truth-machine>

This book provides a detailed account of the creation of the polygraph, arguments surrounding its utilization, and its continued use in an era of other credibility assessment technologies, such as functional magnetic resonance imaging (fMRI). The author also draws from his personal experience as a psychologist to test validity assumptions related to polygraph examination results.

Bushway, Shawn D., Paul Nieuwbeerta, and Arjan Blokland, "The Predictive Value of Criminal Background Checks: Do Age and Criminal History Affect Time to Redemption?" *Criminology*, Vol. 49, No. 1, 2011, pp. 27–60.
<https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1745-9125.2010.00217.x>

This article examines the question of how long individuals convicted of criminal offenses remain likely to reoffend and seeks to identify at which point in time the probability of these former criminals to reoffend falls to the level of those who have never committed a criminal act. This article uses data from a group of Dutch offenders to determine whether the age of last conviction and total number of prior convictions affect the length of time in which the individuals are likely to reoffend. The study finds that young, amateur offenders are “redeemed” after they have abstained from crime for ten years, while older offenders have a shorter period of time before they can be considered redeemed. The study found that the more criminal convictions an individual has, the more time it takes to leave a life of crime behind for good, with some never reaching “redemption.” Those who do reach a point at which they are no longer at risk for reoffending do so only after abstaining from engaging in crime for at least 20 years.

Cohen, Sheldon I., "Use of the Polygraph in Security Clearance Investigations," in *Security Clearances and National Security Information: Law and Procedures*, Monterey, Calif.: Defense Personnel and Security Research Center, December 2000, pp. 62–68.
<https://apps.dtic.mil/dtic/tr/fulltext/u2/a388100.pdf>

This chapter focuses on the history and use of the polygraph to aid security clearance investigations. It contains important secondary sources that provide DoD with procedures for administering polygraphs (such as DoD Directive 5210.48) and notes how polygraph evidence might be used during Defense Office of Hearings and Appeals processes.³

³ Department of Defense Directive 5210.48, *Credibility Assessment (CA) Program*, Washington, D.C.: U.S. Department of Defense, April 24, 2015, incorporating change 1, effective February 12, 2018.

Employment Screening Resources, “ESR Top Ten Background Check Trends,” webpage, undated.

<http://www.esrcheck.com/Tools-Resources/ESR-Top-Ten-Background-Check-Trends/>

This webpage presents trends in background checks since 2008. The ten trends in background screening for the year 2014 are (1) increasing momentum of the “ban the box” movement, which calls for removing the criminal history question from job applications; (2) human resources concerns over updated U.S. Equal Employment Opportunity Commission guidance on employer use of criminal records; (3) controversy over using commercial criminal databases; (4) more class action lawsuits related to background screening failures or negligence; (5) increased use of firms accredited by the National Association of Professional Background Screeners; (6) prevalence of identity theft and storing of background check information overseas; (7) less use of social network searches in background checks; (8) less use of credit reports; (9) increased use of international background checks; and (10) increased speed and efficiency of background checks thanks to more-advanced technology.

Farrell, Brenda S., U.S. Government Accountability Office, *Personnel Security Clearances: Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations*, testimony before the Select Committee on Intelligence, U.S. Senate, March 7, 2018.

<https://www.gao.gov/products/GAO-18-431T>

The personnel security clearance process across the U.S. government was designated as a high-risk area in January 2018, given the many issues that agencies have been experiencing with the timeliness, management, and integrity of the clearance process. This testimony addresses progress that executive branch agencies had made thus far in enacting reforms to the security clearance process, as well as the extent to which these agencies were meeting timeliness goals and reducing the existing investigative backlog for NBIB. This testimony draws on previous GAO reports from late 2017 on continuous evaluation of clearance holders and clearance reform efforts, which were informed by a review of policy documents, data provided by the agencies, and interviews with key agencies, such as ODNI and NBIB. These reports yielded 12 recommendations for ODNI and director of NBIB, including plans for improving the timeliness of investigations and reducing the backlog. NBIB agreed with all of GAO’s recommendations, while ODNI agreed only with some.

Farrell, Brenda S., U.S. Government Accountability Office, "Personnel Security Clearances: Preliminary Observations on Joint Reform Efforts to Improve the Governmentwide Clearance Eligibility Process," testimony before the Subcommittee on Intelligence Community Management, House Permanent Select Committee on Intelligence, U.S. House of Representatives, July 30, 2008.

<https://www.gao.gov/assets/130/120961.html>

Given the history of delays and logjams in processing security clearances, Congress called for a series of reforms to the personnel security clearance process through the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458). The act stipulated that executive agencies must meet certain deadlines for the investigative and adjudicative phases of the security clearance process in order to deliver clearances or rejections in a timely manner. GAO designated DoD as a high-risk entity from 2005 to 2009, given the many delays in, and concerns about the integrity of, the security clearance process. This testimony covers DoD's progress (as of the time of the statement) against the metrics of timeliness and quality. According to the testimony, GAO will continue to monitor DoD's progress in these areas.

Grover, Jennifer, U.S. Government Accountability Office, "Aviation Security: TSA Has Taken Steps to Improve Vetting of Airport Workers," testimony before the Subcommittee on Transportation Security, Committee on Homeland Security, House of Representatives, June 16, 2015.

<https://www.gao.gov/products/GAO-15-704T>

This GAO testimony examines TSA's process for applicant vetting through the Security Threat Assessment. TSA requires applicants requesting unescorted access to secure portions of an airport to go through this process, which includes checks on criminal history, immigration status, and terrorist databases. GAO found that the Security Threat Assessment begins with airport operators collecting applicant information, which is then passed to TSA, which is responsible for conducting an automated check of Federal Bureau of Investigation (FBI) criminal records, adjudicating the immigration and terrorism checks, and sending the results of this criminal history check back to the airport operators for adjudication. The airport operators determine whether anything in an applicant's criminal history might disqualify him or her from TSA employment and eligibility for credentials.

Han, Yuhwa, "Deception Detection Techniques Using Polygraph in Trials: Current Status and Social Scientific Evidence," *Contemporary Readings in Law and Social Justice*, Vol. 8, No. 2, 2016, pp. 115–147.

<https://www.ceeol.com/search/article-detail?id=466425>

This article conducts research in two parts: It first categorizes how U.S. states have used polygraphs as evidence in criminal cases, the legal precedence cited, and the rationale for each admissible result. Second, the article presents a literature review that examines comparison question and guilty knowledge techniques to understand the

state of current research to support the use of the polygraph. The research finds that use of the guilty knowledge technique had a greater “theoretical” foundation and provided jurors with a better understanding of the purpose of the polygraph.

Jaworski, Ryszard, “Further Investigation Supports the Accuracy of Polygraph Examinations,” *Journal of Forensic Identification*, Vol. 56, No. 6, 2006, pp. 913–932. <https://search.proquest.com/docview/194798931?pq-origsite=gscholar>

This article uses three in-depth case studies to validate the use of the control question technique during polygraph examinations. The article suggests that, since results were repeatable throughout each of the case studies examined, continued use of the technique during examinations is warranted.

John, Leslie K., Alessandro Acquisti, and George Loewenstein, “Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information,” *Journal of Consumer Research*, Vol. 37, No. 5, February 2011, pp. 858–873. <https://www.cmu.edu/dietrich/sds/docs/loewenstein/StrangersPlane.pdf>

This article examines consumer decisionmaking and its relation to online purchasing behavior. The article notes that as online marketplaces increasingly shift to assembling big data on customers to target advertising, individuals have become less willing to share personal information. The authors find that if websites attempt to alleviate privacy concerns with various types of preface information on how information may be used, such practices often backfire because individuals may actually feel more concerned about divulging information. Rather, the study finds that “consumers will be especially forthcoming with information when sensitive questions are asked informally,” and “marketers may be particularly successful in obtaining private information when they make the fewest promises to protect consumers’ privacy—enabling marketers to retain great flexibility in how they may use the disclosed information.”

Levashina, Julia, and Michael A. Campion, “Expected Practices in Background Checking: Review of the Human Resource Management Literature,” *Employee Responsibilities and Rights Journal*, Vol. 21, No. 3, 2009, pp. 231–249. <https://link.springer.com/article/10.1007/s10672-009-9111-9>

This article focuses on the importance of preemployment background checks, stating that previous research has demonstrated that many job candidates seriously misrepresent their academic and work credentials. Consequently, the article contends that employers that fail to conduct thorough background checks of potential job candidates may face charges for negligent hiring or employment discrimination. The article draws on the body of literature related to human resource management to define expected practices in background checking, including understanding job requirements, various methods of background checking, thoroughness of the background check, and the role of the application and interview process. The article also uses recent legal cases as examples of what practices are acceptable or potentially legally problematic.

Matthews, Miriam, *Assessing the Use of Employment Screening for Sexual Assault Prevention*, Santa Monica, Calif.: RAND Corporation, RR-1250-AF, 2017.

https://www.rand.org/pubs/research_reports/RR1250.html

This report offers suggestions on how the U.S. Air Force might use particular vetting practices to better address the suitability (proclivity) of recruits to commit sexual assault. The report finds that current Air Force vetting practices would benefit from the use of the Tailored Adaptive Personality Assessment System (TAPAS), which includes topics to address: consideration for others, cooperation, self-control, responsibility, nondelinquency, virtue, and even-temperedness. The report notes that the use of the TAPAS system for all applications could burden Air Force budgets and might best be used only if other indicators are revealed during the course of in-processing.

Metenková, Zuzana, and Jozef Metenko, "The Detection Psychological Manifestations of Non-Verbal Communication by Interrogator," *Procedia-Social and Behavioral Sciences*, Vol. 114, 2014, pp. 564–573.

<https://www.sciencedirect.com/science/article/pii/S1877042813053883>

This research examines the role of nonverbal cues (e.g., hand movements, eye movements, shifting in seat) and their perceived connection to guilt. The article set out to identify both how often law enforcement officers attribute nonverbal cues to guilt and how much those cues are weighted in the overall context of cases. This research did not find conclusive evidence supporting the use of nonverbal cues during interrogations, but it does suggest some ways forward for future nonverbal research.

Miller, Jeanée C., Allison D. Redlich, and Christopher E. Kelly, "Accusatorial and Information-Gathering Interview and Interrogation Methods: A Multi-Country Comparison," *Psychology, Crime and Law*, Vol. 24, No. 9, 2018, pp. 935–956.

<https://doi.org/10.1080/1068316X.2018.1467909>

This research was funded by the FBI's High-Value Detainee Interrogation Group and aimed to compare and contrast interrogation techniques across North America, Europe, Asia, Australia, and New Zealand. The study used a sample of 185 respondents and found that both North American and Canadian interrogation practices were similar (both used a direct accusation approach), whereas Europe, Australia, and New Zealand preferred using an "information-gathering" approach.

Nelson, Raymond, "Testing the Limits of Evidence Based Polygraph Practices," *Polygraph*, Vol. 45, No. 1, 2016, pp. 74–85.

https://www.researchgate.net/profile/Raymond_Nelson/publication/299470504_Testing_the_Limits_of_Evidence_Based_Polygraph_Practices/links/570391a208aedb12706e8d/Testing-the-Limits-of-Evidence-Based-Polygraph-Practices.pdf

This article traces the primary arguments against the use of the polygraph to determine credibility, which include the "reliability, criterion validity, and reproducibility" of test-

ing outcomes. The article suggests that additional research in the areas of “confirmatory testing, statement tests[,] . . . and limits of admitted behavior” may be required to further validate polygraph results.

Office of the Inspector General, U.S. Department of Energy, *Security Clearance Vetting at the Portsmouth Site*, Washington, D.C., February 2016.

<https://www.oversight.gov/report/doe/security-clearance-vetting-portsmouth-site>

This report documents an investigation by the U.S. Department of Energy’s Office of Inspector General into complaints that the contractor Fluor B&W Portsmouth did not fulfill its contractual obligations, as it failed to sufficiently resolve concerns regarding employees’ backgrounds that were uncovered during the preemployment screening process. The Office of Inspector General also looked into the allegation that the background checks required because of the contractor’s negligence could cost the government between \$5,000 and \$15,000 per security clearance granted. The investigation determined that the contractor was not actually legally obligated per the terms of the contract to determine whether an individual was eligible for a security clearance based on adverse information uncovered as part of the hiring process. The Office of Inspector General also found that the contractor was complying with its contractual obligations by conducting preemployment investigative screening of applicants. However, the investigation did reveal that the contractor was not conducting the required reference checks for applicants and thus recommended that Fluor ensure that this requirement is enforced in future.

Office of the Inspector General, U.S. Department of Homeland Security, *Management Alert—CBP Spends Millions Conducting Polygraph Examinations on Unsuitable Applicants*, Washington, D.C., August 2017.

<https://www.oig.dhs.gov/reports/2017/management-alert-cbp-spends-millions-conducting-polygraph-examinations-unsuitable>

This report from the U.S. Department of Homeland Security (DHS) Office of the Inspector General found that Customs and Border Protection had “administered polygraph examinations to applicants who previously provided disqualifying information on employment documents or during the pre-test interview” throughout 2013–2016, spending approximately \$5.1 million on polygraph examinations. The report suggested that, had Customs and Border Protection properly implemented its security interview instrument and adjudicative processes, the agency would have better been able to meet its hiring goals.

Palmatier, John J., and Louis Rovner, "Credibility Assessment: Preliminary Process Theory, the Polygraph Process, and Construct Validity," *International Journal of Psychophysiology*, Vol. 95, No. 1, 2015, pp. 3–13.

<https://www.sciencedirect.com/science/article/pii/S0167876014001354>

This article provides research related to comparison question testing in conjunction with the administration of polygraphs. The article notes that a lack of theoretical literature (specifically, in the related fields of neurosciences and psychophysiology) supporting lines of questioning related to comparison question testing might suggest that the use of concealed information testing and preliminary process theory could strengthen current baseline credibility comparison questions.

Pulice, Erin B., "The Right to Silence at Risk: Neuroscience-Based Lie Detection in the United Kingdom, India, and the United States," *George Washington International Law Review*, Vol. 42, No. 4, 2010, pp. 865–896.

https://heinonline.org/HOL/Page?handle=hein.journals/gwilr42&div=36&g_sent=1&casa_token=&collection=journals&t=1559239631

This article examines the use of neuroscience-based lie detection tests and the legality of its global use. The article traces key differences during the use of these tests, such as measuring "involuntary responses of the brain," which may affect privacy and civil liberty laws and regulations.

Roulin, Nicolas, and Marguerite Ternes, "Is It Time to Kill the Detection Wizard? Emotional Intelligence Does Not Facilitate Deception Detection," *Personality and Individual Differences*, Vol. 137, 2019, pp. 131–138.

<https://www.sciencedirect.com/science/article/pii/S0191886918304689>

This article explores the use of "lie detection wizards," or those practitioners who believe that having a high level of emotional intelligence to detect nonverbal cues is a better predictor of deception. The article cites use several case studies to show that non-verbal cues lack the evidence-based methods needed to show whether individuals are being deceitful.

Stewart, Derek B., U.S. Government Accountability Office, "DoD Personnel Clearances: Delays and Inadequate Documentation Found for Industry Personnel," testimony before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate, May 17, 2007.

<https://www.gao.gov/products/GAO-07-842T>

GAO reviewed data from various agencies and concluded that contractors for the U.S. government waited an average of more than a year to receive Top Secret clearances, despite Office of Management and Budget (OMB) and Office of Personnel Management (OPM) claims to the contrary. GAO analyzed a sample of 2,259 cases and found that the process took an average of 446 days for first-time clearances and 545 days for

updated clearances. The application-submission phase of the security clearance process is supposed to take no more than 14 days, according to stated government goals, but GAO found that, in reality, it takes an average of 111 days. GAO also found that OPM took 286 days, on average, to complete initial investigations for Top Secret clearances, compared with its goal of 180 days. GAO also found that adjudication took 39 days, on average, which is closer to but still exceeds the 30-day requirement that was meant to take effect in December 2006. GAO found that one cause of these delays is under-trained investigators who do not employ technology as they should. Finally, GAO found that these delays may cost the government money and incur additional national security risks.

Strömwall, Leif, and Pär Anders Granhag, "How to Detect Deception? Arresting the Beliefs of Police Officers, Prosecutors and Judges," *Psychology, Crime and Law*, Vol. 9, No. 1, 2003, pp. 19–36.

<https://www.tandfonline.com/doi/abs/10.1080/10683160308138>

This article examines commonly held beliefs among law enforcement officers, lawyers, and judges about deception practices. The authors find that beliefs across these three groups were "remarkably inconsistent" with the literature on mapping actual deception cues (such as nonverbal cues) to deception activities. The article also finds that, contrary to popular belief within these communities, it is easier to detect deception in noninteractive contexts, such as reviewing videotaped questioning.

U.S. Government Accountability Office, *Payday Lending: Federal Law Enforcement Uses a Multilayered Approach to Identify Employees in Financial Distress*, Washington, D.C., 2011.

https://archive.org/stream/242350-federal-law-enforcement-uses-a-multilayered/242350-federal-law-enforcement-uses-a-multilayered_djvu.txt

This report documents the findings of GAO's investigation into payday lending to federal employees in law enforcement and national security positions in three components within DHS (Customs and Border Protect, Immigration and Customs Enforcement, and TSA) and in the FBI. GAO looked into how agencies identify employees who could be security risks because of financial issues (e.g., payday lending) and suggested possible alternatives to payday lending. To conduct this evaluation, GAO reviewed federal policies and procedures governing the collection of financial information and collected data from representatives of the key players in the payday loan industry (e.g., consumer groups and depository institutions).

U.S. Government Accountability Office, *Personnel Security Clearances: Additional Guidance and Oversight Needed at DHS and DoD to Ensure Consistent Application of Revocation Process*, Washington, D.C., 2014.

<https://www.gao.gov/assets/670/665595.pdf>

GAO examined the extent to which DoD and DHS—which grant the highest number of clearances in the executive branch—track data on security clearance–revocation processes, consistently implement government requirements, monitor and oversee these processes, and determine outcomes for employees who have had their security clearances revoked. GAO discovered DoD may have inaccurate data on eligible personnel with access to classified information. In the course of conducting this evaluation, GAO reviewed data from the agencies on security clearance revocation, executive orders, policy documents, and official agency guidance. GAO also conducted interviews with officials from ODNI, DHS, DoD, and the various components of these agencies. GAO recommended that these agencies take measures to improve the quality of their data and implement closer oversight of security clearance–revocation processes. The agencies accepted most of GAO’s recommendations.

U.S. Government Accountability Office, *Security Clearances: Tax Debts Owed by DoD Employees and Contractors*, Washington, D.C., 2014.

<https://www.gao.gov/assets/670/665052.pdf>

GAO examined how many DoD employees and contractors who held or were eligible for all levels of security clearances also held federal debt and found that 83,000 of these employees had more than \$730 million in unpaid federal tax debt as of June 30, 2012. The IRS provided data showing that roughly 40 percent of the 83,000 individuals with federal tax debt had a repayment plan with the IRS as of June 30, 2012. According to DoD, 32 million employees and contractors were granted or deemed eligible for security clearances over the period GAO examined, from January 1, 2006, to December 31, 2011.

U.S. Government Accountability Office, *Criminal History Records: Additional Actions Could Enhance the Completeness of Records Used for Employment-Related Background Checks*, Washington, D.C., February 2015.

<https://www.gao.gov/products/GAO-15-162>

Employers rely on information obtained through FBI criminal history record checks to determine whether a potential employee is eligible to be hired or to obtain a license. The FBI enables access to a nationwide search of state-generated criminal records. In this report, GAO assesses to what degree (1) states conduct FBI record checks for various employment sectors, (2) states have improved the level of completeness of these records, (3) private companies conduct these criminal checks, and (4) there are challenges related to these processes. GAO’s primary recommendation is that the FBI establish timelines and plans to complete the Disposition Task Force’s remaining goals.

The U.S. Department of Justice agreed with all of the GAO recommendations in this report.

U.S. Senate Committee on Homeland Security and Governmental Affairs, "Safeguarding Our Nation's Secrets: Examining the Security Clearance Process," joint hearing before the Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce and Subcommittee on Financial and Contracting Oversight, June 20, 2013.

<https://www.govinfo.gov/content/pkg/CHRG-113shrg82570/html/CHRG-113shrg82570.htm>

This transcript of the joint hearing between the Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce and the Subcommittee on Financial and Contracting Oversight is about current challenges related to the balance between national security and civil liberties. The hearing also addresses how the U.S. government vets federal employees and contractors.

Vrij, Aldert, *Detecting Lies and Deceit: Pitfalls and Opportunities*, 2nd ed., Hoboken, N.J.: Wiley, 2011.

<https://www.wiley.com/en-us/Detecting+Lies+and+Deceit%3A+Pitfalls+and+Opportunities%2C+2nd+Edition-p-9781119965763>

The most recent edition of Aldert Vrij's canonical work (2011) covers the use of (1) behavior analysis, (2) interview methods, (3) statement validity assessment, (4) reality monitoring, (5) scientific content analysis, (6) several different polygraph tests, (7) voice stress analysis, (8) thermal imaging, (9) electroencephalography (EEG), and (10) fMRI. This book serves as a primary resource throughout the defense and intelligence communities.

Wolter, Felix, and Peter Preisendorfer, "Asking Sensitive Questions: An Evaluation of the Randomized Response Technique Versus Direct Questioning Using Individual Validation Data," *Sociological Methods and Research*, Vol. 42, No. 3, August 2013.

<https://journals.sagepub.com/doi/10.1177/0049124113500474>

This article evaluates the randomized response technique in the context of eliciting truthful responses to sensitive-information requests in surveys. The article finds that direct questioning provided more-valid responses for sensitive questions and discounted the effect of randomized response techniques to obtain valid answers.

Zhong, Linda R., and Mark R. Kebbell, "Detecting Truth, Deception, and Innocence in a Mock Counter-Terrorism Scenario: The Use of Forced-Choice Testing," *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 13, No. 1, 2018, pp. 80–92.

<https://doi.org/10.1080/18335330.2018.1438640>

This research sought to test whether the use of forced-choice testing could provide insight into detecting deception in an experimental situation. The researchers conducted

a test using three groups (“witnesses,” “terrorists,” and “innocent individuals”), with the assumption that terrorists would provide the most-deceptive answers. Although the witness and terrorist groups received information regarding a mock attack, the innocent individual group received no information regarding the scenario. The study found that both the terrorist group and the innocent-individual group scored at a similar rate, suggesting diminished utility of the forced-choice testing to detect deception.

Privacy, Civil Liberties, and Legal Concerns

Berkelaar, Brenda L., “Cybervetting, Online Information, and Personnel Selection: New Transparency Expectations and the Emergence of a Digital Social Contract,” *Management Communication Quarterly*, Vol. 28, No. 4, 2014, pp. 479–506.
<https://journals.sagepub.com/doi/pdf/10.1177/0893318914541966>

This article suggests the use of a modified “digital social contract,” whereby organizations provide the context, and periodic open-source checks are conducted to provide transparency on the preemployment process. The article indicates that maintaining this method of transparency and communication will strengthen the relationship between the organization and the prospective employee.

Huth, Carly L., “The Insider Threat and Employee Privacy: An Overview of Recent Case Law,” *Computer Law and Security Review*, Vol. 29, No. 4, 2013, pp. 368–381.
<https://rampages.us/keckjw/wp-content/uploads/sites/2169/2015/02/20130000The-insider-threat-and-employee-privacy-An-overview-of-recent-case-law.pdf>

This article applies case law to ongoing work conducted within the CERT Insider Threat Center, at Carnegie Mellon University, on employee privacy within the workplace. The article makes four key goals for monitoring programs: (1) maintaining transparency with the workforce being monitored, (2) creating an enforceable policy, (3) incorporating changes in technology into the enforceable policy, and (4) considering the reasonableness of the monitoring.

Office of the Inspector General, U.S. Department of Defense, *DoD Security Clearance Adjudication and Appeal Process*, Washington, D.C., Report No. 04-INTEL-02, December 2003.
<https://fas.org/sgp/othergov/dod/dodig1203.pdf>

This report by DoD’s Office of the Inspector General explores the discrepancy between how contractor personnel and DoD civilian employees or members of the military are treated in the security clearance adjudication and appeal processes. This has become a policy issue because contractors are allegedly given more due-process rights than federal employees, and the two groups have separate adjudication and appeal processes. The report recommends establishing a single security clearance adjudication and appeals

process for both groups to enable more-consistent application of adjudicative criteria and make the process more efficient.

U.S. Government Accountability Office, *Privacy: OPM Should Better Monitor Implementation of Privacy-Related Policies and Procedures for Background Investigations*, Washington, D.C., GAO-10-849, September 2010.
<https://www.gao.gov/products/GAO-10-849>

In this report, GAO was tasked with documenting the protective measures that the OPM Federal Investigative Services (FIS) takes to protect personally identifiable information (PII) as it conducts background checks. GAO collected relevant information from each investigative instance in which PII is gathered: questionnaire submissions, scheduling of appointments, investigation, and review. GAO found that OPM did not require risks to PII to be analyzed or mitigated per the E-Government Act of 2002's privacy impact assessment mandate (Pub. L. 107-347). Therefore, OPM could not "be sure that potential risks associated with the use of PII in its information systems have been adequately assessed and mitigated." Additionally, although FIS "tracks PII that is provided to and received from field investigators," it did not monitor "investigators' adherence to its policies and procedures for protecting PII while investigations" were conducted.

U.S. Office of Government Ethics, "The Standards of Conduct as Applied to Personal Social Media Use," Washington, D.C., LA-15-03, April 9, 2015.
[https://www.oge.gov/web/oge.nsf/0/16D5B5EB7E5DE11A85257E96005FBF13/\\$FILE/LA-15-03-2.pdf](https://www.oge.gov/web/oge.nsf/0/16D5B5EB7E5DE11A85257E96005FBF13/$FILE/LA-15-03-2.pdf)

This legal advisory examines the use of social media by U.S. executive branch employees and agencies and applicable standards of conduct for social media under 5 C.F.R. 2635. The U.S. Office of Government Ethics frequently receives questions from federal employees (and their respective agencies) regarding the use of social media despite the information contained within the Code of Federal Regulations. Therefore, this document presents commonly asked questions and further explains the stipulations of the Code of Federal Regulations.

Vromana, Margaret, and Karin Stulz, "Employer Liability for Using Social Media in Hiring Decisions," *Proceedings: Advances in International Interdisciplinary Business and Economics*, Vol. 3, 2016.
https://www.researchgate.net/publication/305729785_Employer_Liability_for_Using_Social_Media_in_Hiring_Decisions

This paper discusses the legal implications involved for businesses searching for open-source information on prospective employees. The paper explains that businesses can run into trouble even when searching for "legitimate" information, since social media sites can contain information on race, religion, and gender identification. The article also discusses how to reduce company liability under state and federal statute.

Yarbrough, Jillian R., "Is Cybervetting Ethical? An Overview of Legal and Ethical Issues," *Journal of Ethical and Legal Issues*, Vol. 11, 2017.

<http://www.aabri.com/manuscripts/172677.pdf>

This article reviews existing literature on cybervetting, provides an overview of how organizations currently deploy cybervetting tools during the initial stages of hiring decisions, and examines some of the potential legal and ethical challenges for hiring managers. The author also presents recommendations for managers.

Adjudication and Adjudication Bias

Adjudicative decisions for security clearances are instituted through the use of 13 specific guidelines found in the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (32 C.F.R. 147). Suitability adjudication decisions follow a separate set of regulations contained in 5 C.F.R. 731.202. There are additional adjudicative guidelines for Top Secret and Sensitive Compartmented Information, which are included under Intelligence Community Policy Guidance 704.2, *Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*.¹ In case law, there have also been numerous challenges of security and suitability decisions.

This chapter includes selected literature related to the vetting stage of adjudication, beginning with guidelines and practices. It also includes literature related to adjudication bias. Initially, we sought to understand what literature indicated about whether personal biases may affect adjudication end processes, but a lack of literature relating bias to adjudication made that difficult. The literature revealed a single report focused on a measurement tool called the Review of Adjudication Documentation Accuracy and Rationales (RADAR) that intended to assist with regulating adjudication decisions, but we were unable to find empirical research related to the tool's effectiveness. Therefore, this chapter focuses on the types of bias that can affect overall decisionmaking and, in one particular case, the evolution of analytical bias that has affected intelligence community assessments over the past 15 years. This chapter concludes with a brief overview of canonical judicial cases that have already affected—or have the potential to affect—vetting policy considerations with regard to adjudication, in particular.

¹ Intelligence Community Policy Guidance 704.2, *Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*, Washington, D.C.: Office of the Director of National Intelligence, October 2, 2008.

Adjudication Guidelines and Practices

Defense Personnel and Security Research Center, *Adjudicative Desk Reference: Assisting Security Clearance Adjudicators, Investigators, and Security Managers in Implementing the U.S. Government Personnel Security Program, Version 4*, Monterey, Calif., March 2014.

https://www.dhra.mil/Portals/52/Documents/perserec/ADR_Version_4.pdf

This adjudicative desk reference was published by the Defense Personnel and Security Research Center (PERSEREC) at the recommendation of the Security Executive Agent Advisory Committee to serve as an adjudicative resource compendium for “personnel security adjudicators, investigators, and managers.” Although the reference is not presented as official adjudication policy, it contains a wealth of background information about how adjudicative processes have evolved over the past decade.

Nelson, Leissa C., Christina M. Hesse, Shannen M. McGrath, and Donna L. Tadle, *2016 RADAR Adjudication Quality Evaluation*, Monterey, Calif.: Defense Personnel and Security Research Center, April 2018.

https://www.dhra.mil/Portals/52/Documents/perserec/reports/MR-18-03_RADAR_2016_Adjudication_Quality_Evaluation_Report.pdf

In 2005, GAO designated the DoD personnel security clearance program as high risk because of its poor performance in terms of timeliness and issues with metrics about the regulation of adjudication quality. DoD has since tried to address this issue through several initiatives, including the RADAR tool, which seeks to align final adjudication results with national adjudication guidelines. To ensure that adjudication decisions are being made and documented correctly, DoD conducts evaluations nearly once a year using RADAR. This report provides the RADAR evaluation results for 2016, which illustrate that 94.6 percent of adjudication determinations were consistent with national adjudication guidelines, though there were also clear areas for improvement. For instance, only 70.5 percent of cases met documentation standards, and many of those that did not meet the standards were missing notations, indicating that previously adjudicated information had been reviewed.

Security Executive Agent Directive 4, *National Security Adjudicative Guidelines*, Washington, D.C.: Office of the Director of National Intelligence, June 8, 2017.

<https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf>

This security executive agent directive establishes a single set of “common adjudicative criteria for all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.” These adjudicative guidelines took effect across the government in June 2017 and apply to any executive branch agency that is either authorized or designated to conduct adjudications for such covered individuals.

Youpa, Daniel G., Jessica A. Baweja, Divya R. Vargheese, Leissa C. Nelson, and Susan C. Reed, *Tier 1 and Tier 3 eAdjudication Business Rule Validation*, Monterey, Calif.: Defense Personnel and Security Research Center, TR-18-06, April 2018.
https://www.dhra.mil/Portals/52/Documents/perserec/reports/TR-18-06_Tier_1_and_Tier_3_eAdjudication_Business_Rule_Validation.pdf

For more than a decade, PERSEREC worked on developing business rules for electronic adjudication (eAdjudication) of security clearances and other types of background screening. eAdjudication has enabled lower costs for adjudication and more-consistent adjudication results than adjudication completed by humans. eAdjudication was initially developed to apply to National Agency Check with Local Agency and Credit Check investigations but has moved toward investigations associated with Tiers 1 and 3 investigations and Tier 3 reinvestigations. PERSEREC has collaborated with other agencies to try to establish eAdjudication as a shared service across the executive branch. This report provides an overview of the business rules for OPM's Tier 1, Tier 3, and Tier 3 reinvestigations products and validates that Tier 1 eAdjudication business rules could "successfully eAdjudicate both Suitability and Homeland Security Presidential Directive 12 case types." The business rules received the approval of the executive agents in March 2017.

Adjudication Bias

Aftergood, Steven, "Secrecy News: Security Clearance Denials and Constitutional Rights," Federation of American Scientists, September 3, 2013.
<https://fas.org/blogs/secrecy/2013/09/hegab-cert/>

This article examines the question of whether judicial review of denied or revoked security clearances is permissible under the Constitution in cases in which an individual claims that discrimination was involved. The article provides a brief overview of some recent legal cases regarding people who had been stripped of their clearances or denied a clearance and attempted to sue the issuing federal agency, concluding that, thus far, there seems to be no viable legal precedent for judicial review of security clearance determinations.

Bond, Charles, and Bella DePaulo, "Individual Differences in Judging Deception: Accuracy and Bias," *Psychological Bulletin*, Vol. 134, No. 4, 2008, pp. 477–492.
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.879.8829&rep=rep1&type=pdf>

This article examines differences in detecting deception by questioners in "real time" without additional aid or information. Using psychometric analysis on a sample of 247 people, the researchers find only "minute" differences between the individual techniques used and that lie detection in this context is less than 1 percent. The article concludes, "When judging deception, people differ less in ability than in the inclina-

tion to regard others' statements as truthful," and "results reveal that the outcome of a deception judgment depends more on the liar's credibility than any other individual difference."

Henkel, Eric, "Say What? How Unconscious Bias Affects Our Perceptions," Nonprofit Risk Management Sector, undated.

[https://www.nonprofitrisk.org/resources/e-news/](https://www.nonprofitrisk.org/resources/e-news/say-what-how-unconscious-bias-affects-our-perceptions/)

[say-what-how-unconscious-bias-affects-our-perceptions/](https://www.nonprofitrisk.org/resources/e-news/say-what-how-unconscious-bias-affects-our-perceptions/)

This article argues that individuals can experience bias on an unconscious level that affects how absorbed information is processed and stored. The article explains that there are a few main types of cognitive processes by which bias can occur: (1) confirmation bias (only accepting information that confirms prior belief), (2) the "false consensus effect" (thinking that others agree with belief systems even though they do not), (3) self-serving bias (attributing success based on personal character traits), and (4) fundamental attribution errors (decisions based on factors related to individual characteristics as opposed to considering other external factors).

Rebugio, Aries B., "Bias and Perception: How It Affects Our Judgment in Decision Making and Analysis," *Small Wars Journal*, July 12, 2013.

<https://www.scribd.com/document/183174946/Small-Wars-Journal-Bias-and-Perception-How-It-Affects-Our-Judgment-in-Decision-Making-and-Analysis-2013-07-12>

This article from the *Small Wars Journal* uses a case study to illustrate how personal bias can affect intelligence collection and assessments. The case study, which includes an extensive literature review on different types of analytical bias, draws heavily from different experiences of intelligence analysts from the Cold War to the present. For example, the article finds that, in the 1980s, "the single most point of failure within the community was the practice of 'risk aversion.'" Further, mirror imaging and rationale actor methods were incorporated into analysis, which prevented alternative views for understanding new information or viewpoints.

Adjudication Legal Concerns

***Greene v. McElroy*, 360 U.S. 474, 1959; *Department of the Navy v. Egan*, 484 U.S. 518, 1988; *Webster v. Doe*, 486 U.S. 592, 1988; *Perez v. FBI*, *Perez v. FBI*, 714 F. Supp. 1414, W.D. Tex., 1989; *Makky v. Chertoff*, 541 F.3d 205, 3d Cir., 2008; *El-Ganayni v. United States DOE*, 2008 U.S. Dist., W.D. Pa., 2010; and *Berry v. Conyers and Northover*, 692 F.3d 1223 (Fed. Cir. 2012), reh'g en banc granted, opinion vacated, 497 F.App'x 64 (Fed. Cir. 2013), and rev'd and remanded sub nom.**

There have been multiple challenges to security and suitability adjudication decisions. In *Greene v. McElroy* (1959), the Supreme Court found that, without "explicit autho-

rization to the contrary, a cleared contract employee could not lose his job unless the proceeding that purported to strip his clearance allowed for confrontation.” In *Department of the Navy v. Egan* (1988), the Supreme Court held that decisions to revoke or deny a clearance is not judicially reviewable and is best left to the executive branch. In *Webster v. Doe* (also 1988), the Supreme Court argued that security clearances revoked in violation of a constitutional right could be reviewable by the judicial branch. These two cases suggest that either a denial or revocation of a clearance might be reviewable only if the defendant can validate that constitutional rights were violated. *Makky v. Chertoff* (2008), *El-Ganayni v. United States DOE* (2010), and *Perez v. FBI* (1989) offer additional clearance appeals. The first two cases reveal the difficulty that courts face when they are asked to review clearance revocations while not actually being able to view the department or agency merits of dismissal, while the third case considered the importance of equal opportunity and civil rights claims. In *Berry v. Conyers and Northover* (combined appeals in 2012), the Circuit Court limited Civil Service Reform Act protections for any federal position that the executive branch deemed as “sensitive,” whether a security clearance is needed to do the job or not (i.e., “sensitive position” and “security clearance” are equated in terms of national security concern or significance). The Circuit Court here combined two separate appeals from the Merit Systems Protection Board, one from *Conyers* and one from *Kaplan* (*Kaplan v. Conyers and Northover*, 733 F.3d 1148, Fed. Cir. 2013, cert. denied, 134 S.Ct. 1759, 2014), since they involved the same legal issue on appeal.

Suitability, Fitness, and Contractor Vetting

In 5 C.F.R. 731.101, *suitability* is defined as “determinations based on a person’s character or conduct that may have an impact on the integrity or efficiency of the service.” That section also evaluates whether employees can effectively meet the duties and responsibilities of positions to maintain the hiring agencies’ reputations and missions.¹ *Fitness*, similar to *suitability*, is a DHS term that refers to character and trustworthiness of the individual for the position.

This chapter covers selected literature regarding U.S. government suitability and fitness programs and how OPM’s Position Designation Tool factors into determining sensitive positions with the government, and then concludes with a brief description of contractor-related suitability processes. Although there are extensive government sources for determining suitability and fitness eligibility, the literature pertaining to contractor vetting is sparse. Given the limited availability of contractor vetting policies, federal departments and agencies have struggled to implement adequate protections for such positions. This difficulty is evidenced through several GAO and Office of Inspector General reports referenced in this chapter, and three case studies note where a lack of contractor vetting policy has resulted in security breaches.

¹ Also see 5 U.S.C. 3301; Executive Order 10577, *Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service*, Washington, D.C.: White House, November 23, 1954; and 5 C.F.R. 1.1, 2.1(a), and 5.2. Specifically, 5 U.S.C. 3301 directs consideration of “age, health, character, knowledge, and ability for the employment sought.” Executive Order 10577 (codified in relevant part at 5 C.F.R. 1.1, 2.1[a], and 5.2) directs OPM to examine suitability for competitive federal employment. This part concerns only determinations of suitability—that is, those determinations based on a person’s character or conduct that may have an impact on the integrity or efficiency of the service. Determinations made under this C.F.R. are distinct from decisions made under 5 U.S.C. 3318 and 5 C.F.R. 332.406 or those made under Executive Order 10450, *Security Requirements for Government Employment*, Washington, D.C.: White House, April 27, 1953; Executive Order 12968, *Access to Classified Information*, Washington, D.C.: White House, August 2, 1995; or similar authorities.

Suitability and Fitness Practices

Allen, Charles E., Intelligence and National Security Alliance, “Doing Business with DHS: Industry Recommendations to Improve Contractor Employee Vetting,” testimony before the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, U.S. House of Representatives, February 27, 2018.

https://www.insaonline.org/wp-content/uploads/2018/02/Charles-Allen_Prepared-Testimony-on-DHS-Vetting-27Feb2018.pdf

This congressional testimony addresses inefficiencies in the policies and procedures governing “fitness determinations” of contractors to support components of DHS, including TSA and Customs and Border Protection. Each component of DHS requires contractors to receive a unique fitness determination, even if they already possess a security clearance. Because contractors routinely support several components, this requirement burdens both government and industry with delayed productivity and increased costs—thus hindering the department’s ability to fulfill its mission. The testimony makes several recommendations for mitigating these inefficiencies, including (1) standardizing the suitability and fitness requirements across the department, consistent with the “unity of effort” campaign undertaken by DHS secretaries from both the current and previous administrations; (2) making those requirements publicly available; (3) empowering the department’s chief security officer to determine and implement consistent requirements across the department; and (4) eliminating the requirement to conduct a fitness or suitability assessment on government or contractor personnel who possess a valid, in-scope security clearance.

Department of Defense Instruction 1400.24, *DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees*, Washington, D.C.: U.S. Department of Defense, 2012.

<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/140025/140025v731.pdf>

This comprehensive DoD instruction contains policy and procedures for civilian personnel management within DoD, policies and procedures related to suitability and fitness investigations and adjudication for federal employment, consistent standards to the extent possible, and required suitability reciprocity practices between U.S. government agencies. The DoD instruction draws on information contained within Executive Order 13467, Executive Order 13488, and Executive Order 10450.²

² Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, Washington, D.C.: White House, June 30, 2008; Executive Order 13488, *Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust*, Washington, D.C.: White House, January 16, 2009; and Executive Order 10450, *Security Requirements for Government Employment*, Washington, D.C.: White House, April 27, 1953.

Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, Washington, D.C.: White House, June 30, 2008.

<https://fas.org/irp/offdocs/eo/eo-13467.htm>

Executive Order 13467 established the PAC to enhance alignment between national security investigative and adjudication practices with suitability functions. This executive order also created the Security Executive Agent and the Suitability Executive Agent to develop, implement, and oversee “effective, efficient, and uniform policies and procedures” for their respective security and suitability processes.

Joint Security and Suitability Reform Team, *Security and Suitability Process Reform*, Washington, D.C., December 2008.

https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/reports/joint_security_dec2008.pdf

This report responds to a congressional inquiry regarding the timeliness of security clearance background checks. The report describes how the Joint Security and Suitability Reform Team’s Security, Suitability, and Credentialing (SSC) framework could serve to improve various aspects of the overall SSC process, including better alignment of suitability and security clearance processes, the enabling of the application of consistent standards, and methods to increase the investigation reciprocity throughout the defense community.

Nelson, Leissa C., and Samantha A. Smith-Pritchard, *Baseline Suitability Analysis*, Monterey, Calif.: Defense Personnel and Security Research Center, TR 13-05, July 2013.

<https://www.dhra.mil/Portals/52/Documents/perserec/tr13-05.pdf>

This study sought to identify suitability practices across several DoD services and agencies. The report specifically focused on how suitability was defined and validated, as well as how potential government employees were recruited and vetted. The report states that the majority of suitability tasks occurred during the vetting step—the last stage of the hiring process. Lastly, this PERSEREC study explored how the suitability process might be consolidated within the DoD Consolidated Adjudications Facility.

Office of Management and Budget, *Suitability and Security Process Review: Report to the President*, Washington, D.C., February 2014.

<https://www.archives.gov/files/isoo/oversight-groups/nisp/2014-suitability-and-processes-report.pdf>

This Office of Management and Budget report is a presidentially mandated review of executive branch employees, military service members, and contractor fitness and suitability determinations and security clearance procedures. The purpose of the report was to “assess risks inherent in the current security, suitability, and credentialing pro-

cesses and identify recommended solutions to safeguard our personnel and protect our nation's most sensitive information." The report offers a series of recommendations related to improving the existing SSC process and suggests ways to more efficiently conduct such programs moving forward.

Office of Personnel Management, "Suitability Executive Agent: Position Designation Tool," webpage, undated.
<https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/>

This webpage from OPM offers the Position Designation Tool as a method for federal departments and agencies to assign risk to specific positions within their organizations. The tool contains clickable policy justifications behind decision criteria (the Code of Federal Regulations and other federal regulations) and provides a printable workbook for agencies to develop a score that relates to a five-tier system. Each tier is representative of suitability and national security access considerations. Lastly, the tool provides a reference for the level of investigation required for each position description (e.g., a tier 5 risk to an organization, something that would cause inestimable damage to the national security of the United States, would follow SF-86 protocols, while a position that merited a nonsensitive or no-risk position would follow SF-85 processes).

U.S. Department of Defense, *Department of Defense Suitability and Fitness Guide: Procedures and Guidance for Civilian Employment Suitability and Fitness Determinations Within the Department of Defense*, Washington, D.C., July 28, 2016.
https://www.dhra.mil/Portals/52/Documents/perserec/DoD_Suitability_Guide_Version_1.0.pdf

This DoD guide was issued to further support suitability and fitness practitioners with investigation and adjudication planning decisions for current and future federal civilian suitability and fitness determinations. The guide serves as a master reference document and incorporates relevant OPM and DoD policies and devotes one section to training suitability program managers. Although the guide does not mandate any of the referenced policies (and cannot be cited as authority for denial or revocation of employment suitability or fitness), it does serve as a baseline document for department and agencies to design such programs.

U.S. Department of Homeland Security, *The Department of Homeland Security Personnel Suitability and Security Program*, Washington, D.C., Instruction Handbook 112-01-007, 2009.
<https://www.dhs.gov/sites/default/files/publications/Instruction%20Handbook%20112-01-007%20Personnel%20Suitability%20and%20Security%20Program.pdf>

This instruction is relevant to DHS-covered individuals (e.g., federal employees, applicants, excepted service federal employees, and contractor employees) providing support

to DHS and who require unescorted access to DHS-owned facilities, DHS-controlled facilities, or commercial facilities operating on behalf of DHS. The instruction also covers access protocols for DHS sensitive information platforms and other IT platforms containing national security information. Lastly, the instruction defines minimum standards for the DHS Personnel Suitability and Security Program—but these are subject to change as new policies are implemented.

Contractor Vetting

U.S. Department of Defense, *National Industrial Security Program: Operating Manual*, Washington, D.C., DoD 5220.22-M, February 2006, incorporating change 2, May 18, 2016.

<https://fas.org/sgp/library/nispom/nispom2006.pdf>

The National Industry Security Program (NISP) Operating Manual (NISPOM) provides classified information requirements for government contractors. The NISP was originally created under by Executive Order 12829 and its aperture expanded under Executive Order 13526.³ The National Security Council (the Secretary of Defense is the executive agent for the NISP) periodically updates the NISPOM in relation to providing overall policy direction for the NISP, while the director of the Information Security Oversight Office is responsible for “implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies.”

U.S. Government Accountability Office, *Contract Security Guards: Army’s Guard Program Requires Greater Oversight and Reassessment of Acquisition Approach*, Washington, D.C., GAO-06-284, April 3, 2006.

<https://www.gao.gov/products/GAO-06-284>

This GAO report focuses on the domestic use of contractors as security guards to defend U.S. Army installations. The report notes that the Army had awarded contracts totaling \$733 million to defend 57 Army installations. GAO ultimately found that the Army did not adequately screen its sole contractor provider, which had never provided security guard service before. Moreover, GAO found 89 security guards with significant criminal offenses. Part of the problem was that the contractors were trusted to provide truthful answers on the paperwork that was never vetted.

³ Executive Order 12829, *National Industrial Security Program*, Washington, D.C.: White House, January 6, 1993; Executive Order 13526, *Classified National Security Information*, Washington, D.C.: White House, December 29, 2009.

U.S. Government Accountability Office, *Operational Contract Support: Actions Needed to Address Contract Oversight and Vetting of Non-U.S. Vendors in Afghanistan*, Washington, D.C., GAO-11-771T, June 30, 2011.

<https://www.gao.gov/products/GAO-11-771T>

This GAO report examines how DoD’s contracting officer’s representatives prepare for “their roles and responsibilities and provide adequate contract oversight in Afghanistan”; how DoD, the U.S. Department of State, and the U.S. Agency for International Development “vet non-U.S. firms for links to terrorist and insurgent groups in Afghanistan”; and whether DoD had implemented previous GAO recommendations on similar subjects of inquiry. GAO found that, although DoD had taken some action to prepare the contracting officer’s representatives within Afghanistan, they were not “fully prepared for their roles and responsibilities to provide adequate oversight there.” In addition, although DoD developed training related to management and oversight of contractors within the country, the training was not specific enough to provide situational awareness of local processes. This led to the need to rebuild or repair infrastructure, in several cases.

U.S. Government Accountability Office, *Operational Contract Support: Additional Actions Needed to Manage, Account for, and Vet Defense Contractors in Africa*, Washington, D.C., GAO-16-105, December 2015.

<https://www.gao.gov/products/GAO-16-105>

This GAO study reports on the extent to which U.S. Africa Command (AFRICOM) is able to manage contract support within country and how the command vets non-U.S. contractors and contractor employees. The study found that, while contract support at the headquarters level was adequate, subordinate commands were not adequately staffed to plan or manage the numerous levels of contract support in the field. Although AFRICOM has instituted the use of a “scorecard” to “assess [operational contract support] management capabilities at the subordinate commands against certain standards,” the assessments “have not always been accurate because the standards have not been clearly defined or consistently applied.” Additionally, although AFRICOM conducts “limited vetting of potential non-U.S. contractors” (a.k.a. vendors), it had not “established a foreign vendor vetting process or cell that would preemptively identify vendors who support terrorist or other prohibited organizations.”⁴

⁴ GAO further explained that “AFRICOM has not yet established a foreign vendor vetting cell because while DoD guidance discusses the benefit of a cell, it does not require it or specify under what conditions it would be appropriate. Additionally, DoD sites in Africa use background investigations to determine the trustworthiness of contractor employees with access to DoD facilities. However, not all AFRICOM sites are incorporating additional screening measures, such as biometric screening or counterintelligence interviews, based on the specific risks at each site.”

Insider Threats

Understanding, preventing, and mitigating the effects of insider attacks represent major themes in this chapter. In 2011, Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*,¹ created the National Insider Threat Task Force to assist the executive branch with implementing 26 “minimum standards” that agencies must incorporate to address insider threats. The task force remains the center of gravity for developing insider threat policy and procedures across the whole of the U.S. government.

This chapter includes prominent U.S. policies and, to address insider threats, a sampling of detection and prevention mechanisms that may help combat insider threats. The chapter concludes with a section on emerging avenues that insider threats may target that have important implications for personnel vetting. Although guidance for U.S. insider threat programs is contained within Executive Order 13587 and the 2012 *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*,² definitions for what constitutes an insider threat are largely dependent on the sector examined. One type of insider threat could be viewed through the lens of classified information leakage (e.g., Edward Snowden or Chelsea Manning) or could be of a more violent nature, as in the case of Major Nidal Hassan or Aaron Alexis.³ There are also other examples noted in the literature that might not meet the “threshold” of a major insider attack but have important considerations for vetting. For example, small-scale workplace violence could surface in the form of a disgruntled ex-employee or a personal relationship struggle that could publicly affect the organization’s reputation. Other reports suggest that the insider threat to organizations do not end at the time of employee separation but could occur in the 60 days postseparation

¹ Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, Washington, D.C.: White House, October 7, 2011.

² White House, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, Washington, D.C., November 2012.

³ Even the National Insider Threat Task Force stated that a one-size-fits-all approach cannot account for the breadth of threats across all sectors.

if adequate controls are not in place to prevent reentry (e.g., credentials could remain active or user accounts could be left open).

Insider Threat Practices and Challenges

Defense Personnel and Security Research Center, *Technological, Social and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage*, Monterey, Calif., TR-05-10, 2005.

<https://fas.org/sgp/othergov/dod/insider.pdf>

This report examines multiple trends in the United States and the world to understand the rising threat of the “insider.” Because of the internet and increased international travel, the world is becoming more accessible to more people, thus increasing opportunity for potential insiders to connect with foreign or nefarious entities. In addition to these new opportunities, socioeconomic factors, such as financial instability and gambling addiction, remain a strong motivating force behind workplace theft. As globalization continues to take hold in society, individuals will be able to easily change jobs and even move to a new country, and loyalties to organizations will diminish.

Intelligence and National Security Alliance, Cyber Council, Insider Threat Task Force, *A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector*, Washington, D.C., September 2013.

<https://www.insaonline.org/a-preliminary-examination-of-insider-threat-programs-in-the-u-s-private-sector/>

This report, produced by the Intelligence and National Security Alliance’s Cyber Council, is a preliminary look at insider threat programs within the private sector. Using interview data and subject matter expertise, the authors recommend practices for mitigating insider threats in organizations. The report finds that many programs are technology focused and monitor only suspicious online or network behavior, but effective programs require a governance structure and multidepartmental cooperation and engagement. Another finding shows that companies with the most mature programs have strong support from company executives.

Luckey, David, David Stebbins, Rebeca Orrie, Erin Rebhan, Sunny D. 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, Calif.: RAND Corporation, RR-2684-OSD, 2019.

https://www.rand.org/pubs/research_reports/RR2684.html

This RAND report explores insider threats and continuous evaluation (CE) as a vetting and adjudication process. This report also relays potential cost benefits from CE over current security clearance methods. Lastly, the report offers key findings and

recommendations on CE programs in their current state and potential avenues for increased effectiveness for future programs.

National Insider Threat Task Force, *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards*, Washington, D.C., 2017.

<https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf>

This compendium of best practices was published by the National Insider Threat Task Force as a complement to its 2014 *Guide to Accompany the National Insider Threat Policy and Minimum Standards*. This publication serves several functions, including as an orientation guide for U.S. government departments and agencies and as a planning document to assist organizations in meeting or exceeding the standards identified in Executive Order 13587, from 2011.

Office for the Director of National Intelligence, National Counterintelligence and Security Center, *Summary of Federal Citations for the National Insider Threat Task Force*, Washington, D.C., undated.

https://www.dni.gov/files/NCSC/documents/nittf/Summary_of_Federal_Agencies_Security_Legal_Authorities.pdf

This is a summary document of federal citations for the National Insider Threat Task Force. The document provides summaries for all relevant U.S. Code, executive orders, and presidential national security and homeland security directives. In addition, it includes citation summaries for intelligence community directives, intelligence community standards, and miscellaneous memoranda and regulations across federal agencies.

White House, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, Washington, D.C., November 2012.

<https://fas.org/sgp/obama/insider.pdf>

This is a presidential memorandum on the national insider threat policy and codifies the minimum standards for insider threat programs for the executive branch. The memo lays out a policy to establish, implement, monitor, and report on the effectiveness of insider threat programs and requires the development of an executive branch program for the deterrence, detection, and mitigation of insider threats. It also establishes general responsibilities for departments and agencies and codifies roles and responsibilities.

Woolley, Christopher, Mark D. Troutman, and Paul B. Losiewicz, "Insider Threat: Policy Impact and Overview," white paper, Center for Infrastructure Protection and Homeland Security, George Mason University School of Law, and Cyber Security and Information Systems Information Analysis Center, June 19, 2014.

<https://cip.gmu.edu/wp-content/uploads/2015/09/Insider-Threat-Paper-Final.pdf>

This white paper from researchers at the George Mason University School of Law and the Cyber Security and Information Systems Information Analysis Center reviews relevant case studies to determine the state of U.S. government insider threat policies, legal implications, and potential measures for future program implementation. The paper concludes that no single factor can predict an insider attack and that developing threat profiles should not be solely based on previous actors, such as Edward Snowden or Chelsea Manning. Rather, the paper suggests, even "low level employees can gain access to unprecedented volumes of data and pose a significant security risk." Finally, the paper suggests that law alone cannot be considered a deterrent for potential insiders, but that access restriction, incentives, and making information itself "smarter" can greatly enhance program effectiveness.

Detection and Prevention Mechanisms

Balakrishnan, Balaji, "Insider Threat Mitigation Guidance," SANS Institute, October 2015.

<https://www.sans.org/reading-room/whitepapers/monitoring/insider-threat-mitigation-guidance-36307>

This paper looks at various frameworks for implementing an insider threat program and presents a case study for a hypothetical organization trying to implement an insider threat program. In addition, this paper provides use cases for insider threat activity detection, using a risk-scoring methodology in which each event is scored and then aggregated to identify high-risk events. If several high-risk events occur together, this is a trigger for further investigation.

Band, S. R., D. M. Cappelli, L. F. Fischer, A. P. Moore, E. D. Shaw, and R. F. Trzeciak, *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis*, Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 2006.

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2006_005_001_14798.pdf

This report examines two critical forms of malicious insider threat activities: sabotage of critical information technology systems and espionage. Although these two are sometimes looked at as separate forms of malicious activity, there is significant overlap in the contextual, psychological, organizational, and technical factors that lead individuals down either path. This report creates a model of commonalities and finds that saboteurs and spies both had personal predispositions and environmental stressors that increased risk for attacks, both exhibited behaviors of concern immediately preceding

the event or attack, respective organizations failed to detect or respond to rule violations, and the organization of these insiders lacked physical and electronic access controls that could have prevented attacks.

Behavior Analysis Unit, National Center for the Analysis of Violent Crime, *Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks*, Washington, D.C.: Federal Bureau of Investigation, 2016.

<https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view>

This report, issued by FBI's Behavior Analysis Unit, is a practical guide for identifying, assessing, and managing the threat of future, planned violence. This guide advocates for several detection and prevention techniques, including promoting a culture of shared responsibility to foster an environment in which bystanders can inform threat managers. In addition, the report highlights the need for easy and effective reporting mechanisms.⁴

Bruce, James B., Sina Beaghley, and W. George Jameson, *Secrecy in U.S. National Security: Why a Paradigm Shift Is Needed*, Santa Monica, Calif.: RAND Corporation, PE-305-OSD, November 2018.

<https://www.rand.org/pubs/perspectives/PE305.html>

This RAND document summarizes findings and conclusions regarding the adequacy of the present system governing secrecy in U.S. national security information. The goal of the study was to make recommendations to improve the system that makes, safeguards, and discloses secrets. One key finding offered by the researchers is that efforts to appreciably improve the way secrets are classified, protected, and disclosed will not likely succeed without corresponding improvements in the structure, culture, rules, and technologies of the secrecy paradigm. There is a dedicated section in this document related to leaks and unauthorized disclosures, with the authors finding that a major failing of the current U.S. secrecy paradigm is its mixed performance in the prevention and detection of espionage, along with its inability to consistently deter or apprehend leakers and hold them accountable for their violations of the law. To this end, the report offers a number of recommendations: reducing the large numbers of cleared government and contractor personnel, reducing the large numbers of cleared personnel with access to highly classified information, establishing uncompromising accountability for leaking classified information, and providing robust support for enhancements in U.S. counterintelligence.

⁴ Also see L. Nan and D. Biros, "Identifying Common Characteristics of Malicious Insiders," *Proceedings of the Conference on Digital Forensics, Security and Law*, 2015.

Bruce, James B., and W. George Jameson, *Fixing Leaks: Assessing the Department of Defense's Approach to Preventing and Deterring Unauthorized Disclosures*, Santa Monica, Calif.: RAND Corporation, RR-409-OSD, 2013.

https://www.rand.org/pubs/research_reports/RR409.html

This RAND report assesses the potential effectiveness of the Unauthorized Disclosures (UD) Program Implementation Team established in 2012 under the Office of the Under Secretary of Defense for Intelligence. RAND researchers determined that, although the implementation of the UD Strategic Plan made important progress toward its main objectives, the advances were partial, fragile, and likely impermanent. RAND researchers offered a series of 22 recommendations, including ways to sustain and expand the effort to prevent and counter unauthorized disclosures.

Critical Incident Response Group, National Center for the Analysis of Violent Crime, *Workplace Violence: Issues in Response*, Quantico, Va.: Federal Bureau of Investigation, 2003.

<https://www.fbi.gov/file-repository/stats-services-publications-workplace-violence-workplace-violence/view>

This report from the FBI's Critical Incident Response Group, National Center for the Analysis of Violent Crime, examines issues in workplace violent crime prevention, threat assessment and management, crisis management, critical incident response, research, and legislation. The report's findings are based on a symposium held in June 2002, which drew from a variety of subject-matter experts across sectors. The report concludes with a variety recommendations, including how best to conduct public awareness campaigns and how to develop workplace policies and plans, as well as other legal and legislative considerations.

Defense Personnel and Security Research Center, *Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders; Analysis and Observations*, Monterey, Calif., TR-05-13, 2005.

<https://www.dhra.mil/Portals/52/Documents/perserec/tr05-13.pdf>

This report provides unclassified excerpts from a larger restricted document. The report presents an overview and analysis of incidents that occurred prior to 2003 within U.S. critical infrastructure industries. The final chapter offers implications and recommendations relevant to future critical infrastructure insider threat programs.

Defense Personnel and Security Research Center, *Modeling Insider Threat from the Inside and Outside: Individual and Environmental Factors Examined Using Event History Analysis*, Monterey, Calif., TR-18-14, August 2018.

http://www.dhra.mil/Portals/52/Documents/perserec/reports/TR-18-14_Modeling_Insider_Threat_From_the_Inside_and_Outside.pdf

This recent report from the Defense Personnel and Security Research Center (PERSEREC) focuses on individual risk factors, such as relationship status and level

of education, presenting findings aside from PERSEREC's historical focus on modeling organizational risk factors. Military personnel data from the Defense Manpower Data Center were combined with open-source information gleaned from the U.S. Department of Commerce, Internal Revenue Service, and U.S. Department of Justice. PERSEREC combined individual factors (active duty personnel, pay, demographics, marital status, occupation, pay grade, bonuses, awards and special pay, and ages of dependents) with environmental "predictors" (regional crime rates, economic conditions, and job availability) and then added surrogate measures (unsuitability attrition, subject of a criminal investigation, recorded security incident, and losing access to classified information) to assist in initial scoping. Although the analysis could not fully correlate all predictors with incidents of insider threat, the report points out that incorporating publicly available information proved useful in helping identify at least some measure of incidents.

Intelligence and National Security Alliance, *Insider Threat Workshop Proceedings: Papers and Presentations from the CSIAC Insider Threat Workshop*, Arlington, Va., July 2013.

<https://www.csiac.org/wp-content/uploads/2016/03/CSIAC-Insider-Threat-Report-Proceedings.pdf>

This publication presents Cyber Security and Information Systems Information Analysis Center workshop proceedings related to cases of classified information leaks (specifically, Chelsea Manning, Edward Snowden, and Julian Assange). The proceedings present a paper from the Center for Infrastructure Protection and Homeland Security (George Mason University School of Law) and review trends in tactics and other "remediation steps of interest to cybersecurity professionals." The proceedings also report on emerging technology trends, including cloud computing and mobile devices. Participants were from DoD, academia, state and federal agencies, homeland security, and supporting contractors.

Intelligence and National Security Alliance, *Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation*, Arlington, Va., April 2017.

https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Mind_Insider_FIN.pdf

This report presents a model of behaviors for malicious insiders and explains that certain individuals may possess traits that make them more susceptible to malicious acts. When these traits mix with environmental stressors, the potential for malicious acts increases. Analyzing this combination of personality traits and environmental stressors can assist in creating an early-warning system for malicious insiders. Combining the modeling of behaviors with monitoring tools and taking a holistic approach to cooperation and sharing of information throughout an organization can also be effective in early detection and prevention.

Intelligence and National Security Alliance, *An Assessment of Data Analytics Techniques for Insider Threat Programs*, Arlington, Va., July 2018.

https://www.insaonline.org/wp-content/uploads/2018/08/INSA_Insider-Threat_Data-Analytics-July-2018.pdf

This assessment of data analytics techniques for insider threat programs by the Intelligence and National Security Alliance provides a framework to evaluate the merits of different techniques. It provides a system to organize these techniques, binning them as either descriptive or predictive and traceable or untraceable. The assessment goes on to analyze the six primary techniques used in insider threat programs and makes the following recommendations: (1) Integrate data analytics into their risk management methodologies; (2) assess which analytic techniques are likely to be most effective given the available data, their organizational structure and culture, and their levels of risk tolerance; (3) evaluate the myriad software tools that evaluate data using the chosen approach; and (4) assess the human and financial resources needed to launch a data analytics program, including the expense of software tools and the training and time needed to structure data, apply tools, and execute a data analytics initiative over time.

Intelligence and National Security Alliance, Insider Threat Subcommittee, *The Use of Publicly Available Electronic Information for Insider Threat Monitoring*, Arlington, Va., January 2019.

<https://www.insaonline.org/wp-content/uploads/2019/02/FINAL-PAEI-whitepaper.pdf>

This report argues that the U.S. government must address the use of publicly available electronic information (PAEI)—specifically, social media and commercially available databases—for personnel security determinations and insider threat purposes. Defined as *information that is available to the public on an electronic platform, such as a website, social media site, or database (whether for a fee or not)*, PAEI can provide insights into an individual's perceptions, plans, intentions, associations, and actions. These data can help employers determine whether employees pose a potential threat to themselves or the organizations. Criteria for evaluating social media may be particularly difficult to establish, both because social media postings might not clearly indicate potential security risks and because social media monitoring by an employer might be seen as overly intrusive. The report recommends the Director of National Intelligence, as the government's Security Executive Agent, work with DoD, which will assume government-wide investigation and adjudication responsibilities, to take several key steps: (1) Determine what sources of publicly available information are relevant to security determinations; (2) develop a single legal interpretation of what PAEI, including social media data, may be collected and analyzed for personnel security purposes; and (3) establish policies for how PAEI, including social media data, may be used for security-related personnel determinations. To do so, the government must determine what PAEI constructively informs a risk assessment, what types are appropriate to use, and how to use such data to make both initial and ongoing assessments.

Interagency Security Committee, U.S. Department of Homeland Security, *Violence in the Federal Workplace: A Guide for Prevention and Response*, Washington, D.C., 2013.

<https://www.dhs.gov/sites/default/files/publications/ISC%20Violence%20in%20the%20Federal%20Workplace%20Guide%20April%202013.pdf>

This report from DHS begins with an analysis of Bureau of Labor Statistics data from 2006 to 2010, which finds that an average of 551 workers per year were killed as a result of work-related homicides. Other statistics provided by DHS find that shootings account for 78 percent of workplace homicides; 83 percent of these shootings occurred within the private sector, while only 17 percent of these shootings occurred in government. The report categorizes workplace violence into four bins based on cases reviewed: (1) criminal intent (perpetrator has no legitimate relationship to the agency or its employees), (2) customer/client (perpetrator has a legitimate relationship with the agency), (3) employee-on-employee (perpetrator is a current or former agency employee), and (4) personal relationships (perpetrator usually does not have a relationship with the agency but has a personal relationship with an agency employee). The report then identifies mitigation and response strategies for implementation.

O’Boyle, Ernest H., Donelson R. Forsyth, and Allison S. O’Boyle, “Bad Apples or Bad Barrels: An Examination of Group- and Organizational-Level Effects in the Study of Counterproductive Work Behavior,” *Group and Organization Management*, Vol. 36, No. 1, 2011, pp. 39–69.

<https://journals.sagepub.com/doi/10.1177/1059601110390998>

This article notes that research on counterproductive work behavior has focused specifically on “individual traits and perceptions that enhance or decrease” counterproductive work behavior. The article highlights the need for a “multilevel perspective” that can further counterproductive workplace behavior insight by “acknowledging the nested nature of the individual within the work group.” This article also provides a thorough literature review on previous counterproductive workplace behavior research and proposes a method to test the multilevel counterproductive workplace behavior perspectives offered.

Shaw, Eric, and Laura Sellers, “Application of the Critical-Path Method to Evaluate Insider Risks,” *Studies in Intelligence*, Vol. 59, No. 2, 2015, pp. 41–48.

<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-2/pdfs/Shaw-Critical%20Path-June-2015.pdf>

This article examines insider hostile acts to understand whether there is a “common set of factors and a similar pattern of individual and organizational behavior” across insider threat cases. The article applies “critical-path” analysis, an approach borrowed from business and medical fields to “identify the interrelationships of processes and their most critical and vulnerable points.” The article suggests that this formative work will aid U.S. intelligence officers tasked with foreign institution recruitment activities.

Silowash, George, Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall, and Lori Flynn, *Common Sense Guide to Mitigating Insider Threats*, 4th ed., Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, December 2012.

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf

The fourth edition of the Carnegie Mellon University CERT Program's guide to mitigate insider threats provides an introduction to the topic of insider threats, outlines current trends, and provides insights from the analysis of more than 700 insider threat cases. The guide also describes 19 best practices that an organization should aim to implement to mitigate insider threats. Unlike previous editions, this version codifies the roles of the six major groups of an organization within each best practice. A successful insider threat program would encourage coordination, engagement, and cooperation between an organization's human resources, legal, physical security, information technology, and software engineering groups, as well as data owners.

Spector, P. E., S. Fox, L. M. Penney, K. Bruursema, A. Goh, and S. Kessler, "The Dimensionality of Counterproductivity: Are All Counterproductive Behaviors Created Equal?" *Journal of Vocational Behavior*, Vol. 68, No. 3, 2006, pp. 446–460.

<https://www.sciencedirect.com/science/article/pii/S0001879105001284>

This article suggests that prior counterproductive workplace behavior research has been overly focused on individual characteristics instead of incorporating the various facets of organizational constructs. This article suggests the use of "sub-scales," including abuse toward others, production deviance, sabotage, theft, and withdrawal, to analyze counterproductive workplace behavior relationships within the organization.

Taylor, Paul J., Coral J. Dando, Thomas C. Ormerod, Linden J. Ball, Marisa C. Jenkins, Alexandra Sandham, and Tarek Menacere, "Detecting Insider Threats Through Language Change," *Law and Human Behavior*, Vol. 37, No. 4, 2013, pp. 267–275.

<https://psycnet.apa.org/record/2013-20282-001>

This article examines the cognitive and social challenges that affect an individual engaging in insider threat activity, offering an indirect way of identifying insider threats. In this behavioral study, researchers conducted a simulation to examine differences in language used in emails of participants engaging in insider threat activity. The study found that insiders become more self-focused, showed an increase in negative emotions, and had greater cognitive processing than their coworkers. The study also found that, over time, individuals conducting insider threat activities changed their language to be less uniform relative to their team members.

U.S. Department of Defense, *DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team*, Washington, D.C., undated.

<https://apps.dtic.mil/dtic/tr/fulltext/u2/a391380.pdf>

This report from DoD's Insider Threat Integrated Process Team provides background on and a framework for understanding the insider threat. In addition, it provides a template for action called "Vigilance, Now," which highlights three areas of immediate improvement: awareness, prevention, and deterrence. The report also provides a list of specific recommendations in the areas of policy and strategic initiatives, personnel, training and awareness, deterrence, protection, detection, and reaction and response.

Cloud-Based Insider Threats

Alhanahnah, Mohannad J., Arshad Jhumka, and Sahel Alouneh, "A Multidimension Taxonomy of Insider Threats in Cloud Computing," *Computer Journal*, Vol. 59, No. 11, 2016, pp. 1612–1622.

<https://academic.oup.com/comjnl/article/59/11/1612/2433249>

This article develops a taxonomy of the insider threat to cloud environments toward building more-effective countermeasures. The article also purports that insider threats should be considered along five dimensions: cloud deployment, source of the attack, attack impact, insider attack approach, and susceptible cloud services. The article indicates that future research in this area can use the taxonomy (and associated dimensions) as a basis of classifying cloud-based insider attacks.

Callegati, Franco, Saverio Giallorenzo, Andrea Melis, and Marco Prandini, "Cloud-of-Things Meets Mobility-as-a-Service: An Insider Threat Perspective," *Computers and Security*, Vol. 74, 2018, pp. 277–295.

<https://reader.elsevier.com/reader/sd/pii/S0167404817302134?token=1616D002A036511C004A638A82416DCBDF52DB3D5500FD70BA5A6FF86396BF0982DFCDAE1F60881DC03DA0B31A45E31>

This article notes the emerging concept of the "cloud of things." Although the internet of things represents the interconnectedness between physical servers and "smart" applications that can range from in home and mobile devices (e.g., smart TVs, Alexa, Siri) to more-sophisticated applications found in smart buildings (biometrics), vehicles (telemetry), and critical infrastructure, this article highlights new instances of risk as physical servers increasingly communicate and store sensitive data within the cyber realm.

Yaseen, Qussai, Yaser Jararweh, Brajendra Panda, and Qutaibah Althebyan, "An Insider Threat Aware Access Control for Cloud Relational Databases," *Cluster Computing*, Vol. 20, No. 3, 2017, pp. 2669–2685.

<https://link.springer.com/article/10.1007/s10586-017-0810-y>

This journal article discusses insider threats in relation to the security of cloud service providers. Since cloud relational databases are an emerging technology, the article proposes a model that incorporates security mechanisms to address data migration issues, which is the real-time transference of sensitive data to cloud architectures. This article also discusses the current state of vulnerabilities within cloud-based systems, such as the policy enforcement point (the “key”) and the policy decision point (the “gate”).

Continuous Monitoring and Continuous Evaluation

Continuous monitoring is a process that involves observing daily individual activities, particularly in relation to computer network use. The National Institute of Standards and Technology defines *continuous monitoring* as “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.”¹ Data collected during continuous monitoring observations are gathered for analysis in the postmonitoring period. *Continuous evaluation* is defined by the Office of the Director of National Intelligence (ODNI) as a personnel vetting process to “leverage technology to perform automated records checks for personnel security on a more frequent basis.”² Continuous evaluation takes data from a wide variety of internal and external sources and compares those data with a set of predetermined standards and analyzes them as soon as anomalies are detected to assess whether the activity suggests that the person may pose a security risk.³ Both of these concepts are important in implementing personnel vetting initiatives in the Trusted Workforce 2.0 initiatives and general reform of the personnel vetting processes.

The Security Executive Agent under ODNI established the formal Continuous Evaluation Program within the National Counterintelligence and Security Center in 2008.⁴ Formally, continuous evaluation is a “personnel security investigative process,” and is “part of the security clearance reform effort to modernize personnel security processes and increase the timeliness of information reviewed between periodic reinvestigation cycles.”⁵ The use of continuous evaluation as a tool is meant to bolster currently available investigative methods (e.g., background checks, interviews), not to replace the

¹ National Institute of Standards and Technology, Computer Security Resource Center, *Glossary*, Gaithersburg, Md., undated.

² ODNI, “Continuous Evaluation: Top 15 Frequently Asked Questions,” April 3, 2017.

³ One of this annotated bibliography’s peer reviewers was helpful shaping the distinction we make here between the continuous evaluation and continuous monitoring concepts.

⁴ See Executive Order 13467, 2008.

⁵ ODNI, “Continuous Evaluation—Overview,” webpage, undated.

personnel security processes.⁶ Continuous evaluation can bolster legacy investigative tools through the use of automated records checks to assist federal departments and agencies with the decision to grant a security clearance or with suitability determinations. The National Counterintelligence and Security Center within ODNI provides oversight and guidance for the implementation of continuous evaluation across the U.S. government.

This chapter consists of selected literature regarding U.S. efforts to implement continuous monitoring and evaluation programs (some publications also refer to these as *continuous vetting* programs) and issues with implementation, and the chapter offers literature that can be used to model and analyze information gleaned from the use of such programs. Operationalizing continuous monitoring and continuous evaluation programs have been a goal for the U.S. government since the 1980s. The effectiveness of such programs has mixed success as evidenced by cases within the insider threat section. However, the use of continuous monitoring and continuous evaluation, and insider threat detection, seems to have had recent impact as reported in the recent case of Christopher Paul Hasson, who allegedly used U.S. Coast Guard information systems to research and prepare for an attack.⁷

Federal Risk and Authorization Management Program, *Continuous Monitoring Strategy Guide*, Version 3.2, Washington, D.C.: Office of Management and Budget, April 4, 2018.

https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf

This OMB memo discusses new National Institute of Standards and Technology guidelines developed for continuous monitoring of cloud-based service providers for the U.S. government. The guidelines put forth in this document are a result of a previ-

⁶ There are several ongoing cases regarding the implementation of DoD's Military Accessions Vital to the National Interest (MAVNI) pilot program that intersect with some aspects of continuous evaluation. Although there are other MAVNI cases at the district court level, *Tiwari v. Mattis* (2019) is particularly relevant to this category. The basis of the lawsuit in *Tiwari* is whether applying enhanced procedures to naturalized citizens (who enlisted via MAVNI) violates their constitutional right to equal protection. Most of the other district-level MAVNI cases relate to immigration, but the *Tiwari* case may have consequences on DoD's decision to institute the continuous vetting process. In addition, although DoD's new vetting policy for MAVNI individuals has reached only the district level at this point, this does not mean that it will not at some point potentially circulate up through the circuit courts and possibly even to the Supreme Court. This case was decided in January 2019. Lastly, the district court in the *Tiwari* case issued an injunction against DoD that prohibits it from further applying the MAVNI policy against any other similarly situated service member. In this way, the effect of the decision is department-wide and not limited to those individuals who sued. As of April 2019, DoD filed an appeal with the 9th Circuit to overturn the injunction.

⁷ See Lynh Bui, Dan Lamothe, and Michael E. Miller, "Coast Guard Lieutenant Used Work Computers in Alleged Planning of Widespread Domestic Terrorist Attack, Prosecutors Say," *Washington Post*, February 21, 2019. For more on the level of vetting performed by the U.S. Coast Guard in relation to this case, see Alex Horton, "Immigrant Recruits Face More Scrutiny Than White Supremacists When They Enlist," *Washington Post*, February 21, 2019.

ous OMB memo seeking to move from a “static point in time security authorization processes” to “ongoing assessment and authorization throughout the “system development life cycle.”⁸

Herbig, Katherine L., Ray A. Zimmerman, and Callie J. Chandler, *The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security*, Monterey, Calif.: Defense Personnel and Security Research Center, TR-13-06, November 2013.

<https://apps.dtic.mil/dtic/tr/fulltext/u2/a626819.pdf>

This report discusses the historical development of the Defense Personnel and Security Research Center’s Automated Continuous Evaluation System (ACES). The ACES program began as a way to vet the electronic records submitted during periodic reinvestigations for Secret and Top Secret security clearances, but was expanded (via several pilot programs) to include other types of investigations in the wake of the 2008 Joint Reform Effort.⁹ Since 2008, ACES use has ranged from verifying information provided to agencies on the SF-86 to being a medium to collect additional information from other federal databases.

Insider Threat Subcommittee, Security Policy Reform Council, “Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation,” Washington, D.C.: Intelligence and National Security Alliance, April 2017.

https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Mind_Insider_FIN.pdf

This white paper from the Intelligence and National Security Alliance outlines several considerations for organizations seeking to predict whether certain types of behavior could indicate an insider threat. The Intelligence and National Security Alliance offers a behavioral model construct and applies it to several threat factors, drawn from two of its previous publications, *Leveraging Emerging Technologies in the Personnel Security Process* (which offered ways to continuously evaluate and monitor those accessing sensitive information) and *A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector* (which sought ways to assess and compare industry’s initial implementation of insider threat programs).¹⁰ This paper finds that “less severe counterproduc-

⁸ OMB, “FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,” memorandum, Washington, D.C., April 21, 2010.

⁹ The Joint Reform Effort (led by the Joint Reform Team) was primarily focused on creating efficiency in the U.S. government’s hiring and clearing process for individuals requiring a security clearance. Efforts also centered on creating consistent hiring standards and clearance reciprocity.

¹⁰ Intelligence and National Security Alliance, *Leveraging Emerging Technologies in the Security Clearance Process*, Arlington, Va., March 2014; Intelligence and National Security Alliance, *A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector*, Arlington, Va., September 2013.

tive work behaviors commonly occur before the decision to initiate a major damaging act” and that the “clustering” of such behaviors “into families may help define an “early warning system” and improve understanding of how individual characteristics and environmental factors may mitigate or intensify concerning behaviors.” The Intelligence and National Security Alliance purports that such behavioral clusters could be traced through the use of big data, such as advanced lexical analysis of social media, and other types of sentiment analysis conducted through work email.

Security Executive Agent Directive 6, *Continuous Evaluation*, Washington, D.C.: Office of the Director of National Intelligence, January 12, 2018.

<https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-6-continuous%20evaluation-U.pdf>

This directive establishes policy and requirements for the continuous evaluation of covered individuals (executive branch employees) who require continued eligibility for access to classified information or require eligibility to hold a sensitive position. This foundational document also lays out several definitions, responsibilities, and policies to guide executive agencies in establishing continuous evaluation programs.

Shaw, Eric D., Lynn F. Fischer, and Andrée E. Rose, *Insider Risk Evaluation and Audit*, Monterey, Calif.: Defense Personnel and Security Research Center, TR-09-02, August 2009.

<https://www.nsi.org/pdf/reports/Insider%20Risk%20Evaluation.pdf>

This technical report from the Defense Personnel and Security Research Center discusses a series of effective organizational management techniques in areas of policy, practice, recruitment, preemployment screening, and training and education. The report finds that cultural, political, economic, and other sector-specific factors can “magnify” an insider threat risk, such as cross-cultural differences or even the location of the organization.

U.S. Government Accountability Office, *Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain*, Washington, D.C., GAO-11-149, July 8, 2011.

<https://www.gao.gov/products/GAO-11-149>

This GAO report examines the Department of State’s iPost continuous evaluation program, which seeks to apply automated risk scoring to the department’s IT infrastructure. The two main aims of this report were to understand (1) how the department had “identified and prioritized risk” within the iPost program and (2) how information obtained through the program is applied to making improvements, along with other cost-benefit analyses. Although the program was able to identify security gaps and prioritize them based on the scoring system assigned, implementation has been strained by such factors as finding the right individuals to address the problem once found and “managing expectations” from stakeholders about the comprehensiveness of the tool.

U.S. Government Accountability Office, *Personnel Security Clearances: Plans Needed to Fully Implement and Oversee Continuous Evaluation of Clearance Holders*, Washington, D.C., GAO-18-117, November 21, 2017.
<https://www.gao.gov/products/GAO-18-117>

This report from GAO serves as the unclassified companion to a restricted version of the report examining both ODNI's and DoD's ongoing efforts to establish a government-wide (executive branch) continuous evaluation program. The report also assesses the effectiveness of DoD's and its partner agencies' continuous evaluation pilot programs and the potential cost and time saving element such a program would have on periodic reinvestigations. GAO found that uncertainty regarding how to implement the first phase of the program, such as having a formal policy on what the program would cover, has had a negative ripple effect among several other agencies that have been unable to plan for localized implementation or estimate the costs of running such a program. GAO's primary recommendation is that the ODNI must develop a formalized policy for eventual continuous evaluation implementation, develop the actual implementation plan, and weigh the cost of such a program against resource-strained agencies.

Trust in the Workplace

The Security Executive Agent and the Suitability and Credentialing Executive Agent announced the U.S. government's Trusted Workforce 2.0 initiative in March 2018.¹ The Trusted Workforce 2.0 is an effort aimed at overhauling federal vetting programs and practices. Trusted Workforce 2.0 also intends to develop "near-term actions to significantly reduce the background investigations inventory" and "revamp" the "fundamental vetting approach" through the creation of a new policy framework.² Trusted Workforce 2.0 will likely institute new business process within the Security, Suitability, and Credentialing (SSC) community and modernize much of the IT infrastructure currently used to support investigations and adjudications. A March 2018 Cross Agency Priority briefing, which provides regular updates on the implementation of the President's Management Agenda, defined the theory of change for Trusted Workforce 2.0 thusly: "successfully moderniz[ing] our processes . . . [by] developing agile capabilities that integrate the latest innovative technologies to facilitate continuous vetting of more of our trusted workforce and promote delivery of real-time information to the appropriate SSC professional responsible for making risk-based decisions."³ Both ODNI and OPM are tasked by the Performance Accountability Council to provide recommendations "for the expansion of continuous vetting across the entire Federal workforce to regularly review their backgrounds" to determine whether they will continue to meet applicable requirements.⁴

This chapter includes selected literature regarding the Trusted Workforce 2.0 initiative, noted best practices for considering trust in the context of organizational workforces, and how academic trust modeling can be incorporated into U.S. government planning sessions, as well as other publications that examine how certain per-

¹ Lauren Girardin, "Can Trusted Workforce 2.0 Fix Government's Security Clearance Woes?" GovLoop.com, April 2, 2018.

² President's Management Agenda, *Security Clearance, Suitability/Fitness, and Credentialing Reform*, Washington, D.C., 2018.

³ President's Management Agenda, 2018.

⁴ President's Management Agenda, 2018.

sonality traits may correlate to trust. Identifying personality traits that might reveal a future lack of trust can be difficult. No single trait can qualify as a predictor of trust. Further, much of the literature below notes the importance of establishing longitudinal research designs to develop distinct trust case studies. Cross-sectional research in the field of trust can be problematic, since it reveals only a snapshot and does not allow for the consideration for additional factors, such as major decision points, or other causalities that might have accounted for decreases in trust. Lastly, this chapter draws on literature about how organizations might institute trust-building measures with their employees, which could assist in mitigating potential insider attacks.

Trust in the Workforce

Henshel, D., M. G. Cains, B. Hoffman, and T. Kelley, "Trust as a Human Factor in Holistic Cyber Security Risk Assessment," paper presented at the 6th International Conference on Applied Human Factors and Ergonomics 2015 and the Affiliated Conferences, Las Vegas, July 2015.

https://www.researchgate.net/profile/Diane_Henshel/publication/283960105_Trust_as_a_Human_Factor_in_Holistic_Cyber_Security_Risk_Assessment/links/58cc8f384585157b6dac12f3/Trust-as-a-Human-Factor-in-Holistic-Cyber-Security-Risk-Assessment.pdf

This research states that, to develop a "holistic, predictive cyber security risk assessment model," human behavior is "needed to understand how the actions of users, defenders, and attackers affect cyber security risk." The authors argue that "trust" should be the main indicator for human factors, while "confidence" should be reserved for IT systems. The research suggests that this dual approach allows both internal (personal) and external (systems) situational factors to be considered for future trust modeling.

Intelligence and National Security Alliance, "Building a 21st Century Trusted Workforce," transcript, National Security Institute at George Mason University, Arlington, Va., October 30, 2018.

<https://www.insaonline.org/wp-content/uploads/2018/11/Building-A-21st-Century-Trusted-Workforce-Transcript.pdf>

In October 2018, George Mason University's National Security Institute hosted a seminar regarding the U.S. government Trusted Workforce 2.0 initiative. This document provides a transcript of the discussion between Senator Mark Warner (vice chairman, Senate Select Committee on Intelligence), Susan Gordon (principal deputy director of national intelligence, ODNI), Kevin Phillips (CEO and president, ManTech), and Letitia Long (Chairman, Intelligence and National Security Alliance).

Mayer, Roger C., James H. Davis, and F. David Schoorman, "An Integrative Model of Organizational Trust," *Academy of Management Review*, Vol. 20, No. 3, 1995, pp. 709–734.

<https://www.jstor.org/stable/pdf/258792.pdf>

This article examines the role of trust in organizations through the presentation of a new organizational risk model. This model incorporates three factors of perceived trustworthiness (ability, benevolence, and integrity), individual measures of propensity to trust, and elements of risk-taking within a trusted relationship. The study finds that trusting individuals to perform one specified task might not be transferrable to other tasks and should be considered through the lens of the model proposed.

Raskin, David, Charles Honts, and John Kircher, *Credibility Assessment: Scientific Research and Applications*, Cambridge, Mass.: Academic Press, 2014.

<https://www.elsevier.com/books/credibility-assessment/raskin/978-0-12-394433-7>

This textbook from Elsevier combines subject-matter expertise in the areas of polygraph testing, biometrics, and psychology. The book describes the theory and practice behind several types of deception detection currently deployed globally (fMRI, ocular-motor metrics, and other behavioral and facial monitoring programs), their current utility, and prospects for incorporating future technology.

Yip, Jeremy A., Maurice E. Schweitzer, and Samir Nurmohamed, "Trash-Talking: Competitive Incivility Motivates Rivalry, Performance, and Unethical Behavior," *Organizational Behavior and Human Decision Processes*, Vol. 144, January 2018, pp. 125–144.

<https://www.sciencedirect.com/science/article/pii/S0749597816301157>

This research was conducted through a series of five experiments. The authors find that “trash-talking” coworkers can fuel competition in the workplace, since the targets of trash-talking were “particularly motivated to punish their opponents and see them lose.” This research also finds that the targets of trash-talking were more likely to “cheat” during competitions and likely stymied creative behaviors.

Modeling Trust

Bodnar, Todd, Conrad Tucker, Kenneth Hopkinson, and Sven G. Bilén, "Increasing the Veracity of Event Detection on Social Media Networks Through User Trust Modeling," *Proceedings of the 2014 IEEE International Conference on Big Data*, 2014.

https://www.researchgate.net/publication/268147653_Increasing_the_Veracity_of_Event_Detection_on_Social_Media_Networks_Through_User_Trust_Modeling

This article considers the veracity of social media information against the lens of trust modeling. The article develops a “veracity assessment model” for information gleaned

from social media sites (Twitter and Facebook data), combining the use of a “natural language processing” and “machine learning algorithm” to data mine “textual content generated by each user.” The article uses four case studies to research how certain types of information (and misinformation) are communicated. Results show that the metadata tied to each individual can “provide significant insight on the social media network’s users’ tendency to accurately discuss a topic” 75 percent of the time for the cases used.

Cho, Jin-Hee, Kevin Chan, and Sibel Adali, “A Survey on Trust Modeling,” *ACM Computing Surveys*, Vol. 48, No. 2, 2015.

https://www.researchgate.net/profile/Jin_Hee_Cho4/publication/283670108_A_Survey_on_Trust_Modeling/links/56686b8a08ae7dc22ad36bd7.pdf

This research derives from author-stated methodological insufficiencies on how to “model and quantify trust with sufficient detail and context-based adequateness.” Previous modeling work has suffered from certain communication complexities (protocols, information exchange, social interactions, and cognitive motivations). This article then outlines how different components of trust might be mapped against different layers of complex computer networks.

Hang, Chung-Wei, Yonghong Wang, and Munindar P. Singh, “An Adaptive Probabilistic Trust Model and Its Evaluation,” *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems*, Vol. 3, 2008, pp. 1485–1488.

<https://dl.acm.org/citation.cfm?id=1402905>

This paper from a conference on developing trust models and simulations addresses various factors that must be considered when developing conceptual models of trust. The authors believe that much of the modeling completed to date has remained static, excluding avenues to update new behavioral factors during simulation. The article suggests that future trust modeling must find a way to rapidly incorporate behavior changes to provide more-effective predictions.

Other Characteristics of Trust (Personalities and Building Trust)

Fahr, René, and Bernd Irlenbusch, “Identifying Personality Traits to Enhance Trust Between Organisations: An Experimental Approach,” *Managerial and Decision Economics*, Vol. 29, No. 6, 2008, pp. 469–487.

<https://onlinelibrary.wiley.com/doi/abs/10.1002/mde.1415>

This article examines a subset of factors contained within the Sixteen Personality Factor Questionnaire (16 PF-R) to characterize whether preemployment personality tests are indicative of actual workplace behavior. The study suggests that such personality tests are usually specific to an organization’s culture and therefore might not be

readily transferrable across organizations. The authors find that individuals with low anxiety may represent the largest trusted group within organizations, while individuals with low “self-control” values could be characterized as unreliable.

Freitag, Markus, and Paul C. Bauer, “Personality Traits and the Propensity to Trust Friends and Strangers,” *Social Science Journal*, Vol. 53, No. 4, 2016, pp. 467–476.
<https://www.sciencedirect.com/science/article/pii/S0362331915001123>

This article finds that social trust is engrained in specific personality traits. Three specific personality traits—agreeableness, conscientiousness and openness—are important traits for “trust in friends and strangers” and “agreeable people have a higher level of trust in strangers.” The article indicates that, because personality traits are biological and specific to each individual, trust and trustworthiness may even be hereditary. External factors, such as education and social networks, must also be incorporated into future studies.

Hitch, Chris, “How to Build Trust in an Organization,” Chapel Hill: University of North Carolina Kenan-Flagler Business School, 2012.
<https://www.slideshare.net/BusinessEssentials/how-to-build-trust-in-an-organization>

This white paper explains that trust is earned both through action and interaction. The paper illustrates the multiple benefits of attaining trust within an organization, such as achieving higher profits and having a work population that more readily displays ethical behavior and ultimately retaining a talented workforce. This paper also highlights how organizations can develop trust and how to spot the “erosion” of trust in the workplace, and it also offers more-granular steps that human resource personnel can take to rebuild trust within an organization.

Ihsan, Zohra, and Adrian Furnham, “The New Technologies in Personality Assessment: A Review,” *Consulting Psychology Journal: Practice and Research*, Vol. 70, No. 2, 2018, pp. 147–166.
<https://psycnet.apa.org/record/2018-17017-001>

This article explores the validity (and feasibility) of using big data, wearable technology, gamification, video résumés, and automated personality testing to collect information about potential employees in various public and private sectors. Although several organizations are combining data associated with these five areas with application materials, the article finds that, in many instances, potential employees can adopt different personality traits outside the office that are not transferrable to the workplace environment. For example, individuals might be outspoken and socially active outside the workplace but might present as introverted within the workplace. The article also suggests that knowing that a potential employer will be scraping Facebook or Twitter data will often delete profiles and pursue a “dark social media presence” that cannot be captured via current data-scraping tools. To validate future research, the article sug-

gests combining longitudinal open source data in tandem with the development of “dependent measures” of actual positive work behaviors.

Levine, Emma E., T. Bradford Bitterly, Taya R. Cohen, and Maurice E. Schweitzer, “Who Is Trustworthy? Predicting Trustworthy Intentions and Behavior,” *Journal of Personality and Social Psychology*, Vol. 115, No. 3, 2018, pp. 468–494.
<http://psycnet.apa.org/record/2018-33235-001?doi=1>

This article furthers the discussion of trustworthy behavior by examining six other studies that used “economic games” to measure intentions and a variety of other personality traits. The authors identify both an overwhelming sense of guilt (“guilt proneness”) and “interpersonal responsibility” as major underlying mechanisms for predicting character trustworthiness.

Thielmann, Isabel, and Benjamin E. Hilbig, “The Traits One Can Trust: Dissecting Reciprocity and Kindness as Determinants of Trustworthy Behavior,” *Personality and Social Psychology Bulletin*, Vol. 41, No. 11, 2015, pp. 1523–1536.
<https://www.ncbi.nlm.nih.gov/pubmed/26330455>

This article explores personality traits as predictors of trustworthiness within an organization. The article explains that three main “mechanisms” have been proposed in previous literature, including unconditional kindness, positive reciprocity, and negative reciprocity. This article combines these three mechanisms with a separate trait-based approach known as HEXACO (honesty, humility, emotionality, extraversion, agreeableness, conscientiousness, and openness to experience). Findings suggest that unconditional kindness has an exclusive link with honesty and humility.

van der Werff, Lisa, and Finian Buckley, “Getting to Know You: A Longitudinal Examination of Trust Cues and Trust Development During Socialization,” *Journal of Management*, Vol. 43, No. 3, 2017, pp. 742–770.
<https://journals.sagepub.com/doi/abs/10.1177/0149206314543475>

This article reviews previous studies focusing on the development of trust in a workplace environment to develop a longitudinal analysis. The article suggests that workplace trust develops along a linear path during the work socialization process, which can be studied longitudinally. The article confirms that trusting behaviors can develop along different rates of growth, stability, or even decline, in some instances. Lastly, the articles finds that the propensity to trust prior to the socialization stages is a strong predictor of trust during the initial stages of socialization but does not affect ongoing trusted relationship in subsequent stages.

Wilder, Ursula M., "The Psychology of Espionage," *Studies in Intelligence*, Vol. 61, No. 2, June 2017.

<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-61-no-2/pdfs/psychology-of-espionage.pdf>

This article focuses on spies whose espionage appears to be primarily self-interested, rather than altruistic or self-sacrificing. Within this criminal or treasonous type, specific psychological factors commonly occur, providing a guide to understanding the motives, behavior, and experiences of this type of spy. The risk of espionage can be reduced through understanding these psychological patterns and tailoring counter-measures accordingly.

Asset Protection

In regard to asset protection, personnel vetting can be thought of as achieving three specific ends: protecting U.S. critical infrastructure and other sensitive site locations (*places*), including those in the workforce at those locations; protecting sensitive or other hazardous physical items, such as weapons, chemicals, or nuclear materials (*physical assets*); and protecting government information (*information and intellectual property*). U.S. policy in these three areas is abundant, though it does not always draw distinct connections between the importance of vetting, specifically, and the protection of these types of assets. Much of the asset-based vetting issues are tied to the use of OPM's position-designated tool itself; although the tool identifies some risks associated with a particular sensitive position, the tool does not allow planners to fully understand other areas (e.g., vulnerable populations, information servers) that individuals may have access to.

This chapter includes selected literature related to the nexus between personnel vetting and the protection of critical infrastructure, supply-chain management, and the physical security of organizations, providing relevant U.S. policy where available. The literature in this chapter reveals that there is no common asset definition; although intellectual property theft may be important to technological firms, patients or veterans may be the most valuable means of protection for a hospital or U.S. Department of Veterans Affairs (VA) facility. Previous chapters addressed the *people* aspects of personnel vetting. This chapter focuses on the protection of *places* and *things*.¹ Literature in this chapters includes cases in which a lack of oversight contributed to the loss of major weapon platforms and other cases in which the use of foreign contractors meant that there were sensitive-information vulnerabilities in DoD IT architecture. One publication examines the use of existing technology (mobile MRI device) to vet populations with access to nuclear materials. Others suggest that organizational over-reliance on technological measures have placed too much trust in systems that can malfunction, highlighting the importance of modernizing physical-security practices

¹ The literature on people is presented under the insider threat category.

(e.g., guard training, acquiring modern communications equipment, and line-of-sight monitoring).

Places (Critical Infrastructure and Site Locations)

Giannopoulos, Georgios, Roberto Filippini, and Muriel Schimmer, *Risk Assessment Methodologies for Critical Infrastructure Protection, Part 1: A State of the Art*, Luxembourg: Joint Research Centre, European Commission, 2012.

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf

This report provides information on the Joint Research Centre's Institute for the Protection and Security of the Citizen, whose mission is to provide "research results and to support EU [European Union] policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies." The report has various sources of interest, including the European Programme for Critical Infrastructure Protection and the *National Strategy for Critical Infrastructure*.²

Hutter, David, "Physical Security and Why It Is Important," Bethesda, Md.: SANS Institute, 2016.

<https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120>

The SANS Institute, one of the foremost centers for information security training and security certification in the United States, published this paper in 2016 to highlight the importance of physical security within the workplace, since physical security can often be an afterthought when compared with information security. The author finds that physical security is often overlooked by departments and agencies that have become too focused on technology countermeasures. The advent of mobile data storage (laptops, USBs, tablets, and smartphones) has contributed to the problem of maintaining sensitive information security. The paper suggests that organizational assets "need to have a layered approach" to make it "harder for an attacker to reach their objective."

Organisation for Economic Co-operation and Development, *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*, Paris, May 2008.

<https://www.oecd.org/daf/inv/investment-policy/40700392.pdf>

This report from the Organisation for Economic Co-operation and Development reviews definitions of *critical infrastructure* across several different countries, highlight-

² See European Programme for Critical Infrastructure Protection, "Critical Infrastructure," webpage, undated; Government of Canada, *National Strategy for Critical Infrastructure*, Ottawa, 2009.

ing differences and commonalities in understanding what constitutes criticality. This document also reviews how foreign governments have developed policy in response to emerging threats. Some of the key findings include the following: Most national critical infrastructure policies adopt risk management approaches, countries might have one or more investment measures (blanket restrictions or sectoral licensing or contracting or transsectoral measures, such as investment review procedures), and several of the countries have assigned “little or no role to investment policy.”

U.S. Department of Homeland Security, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Washington, D.C., February 2003.

https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

One of DHS’s first major policies after its creation in November 2002 addressed the protection of U.S. critical infrastructure and key assets. This DHS strategy identifies goals, objectives, and principles for guiding protective functions that have continued into the present. The strategy also called for increased collaboration between the government, the public sector, and the private sector to prepare for and identify threats associated with the 16 identified critical infrastructure areas.³

U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, Washington, D.C., 2013.

<https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf>

This document updates policy contained within DHS’s 2003 *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (see previous entry) and the 2009 National Infrastructure Protection Plan.⁴ It specifically discusses progress made with establishing partnerships between federal, state, local, tribal, and territorial governments; regional entities; nonprofit organizations; and academia, all of which continue to play a critical role in managing risks to U.S. critical infrastructure, both physical and cyber. This plan incorporates policy issued under Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, which explicitly calls for an update to the National Infrastructure Protection Plan. It adds the element of cybersecurity (contained within Executive Order 13663) and also incorporates elements of Presidential Policy Directive 8, *National Preparedness*.⁵

³ Also see M. Keeney, E. Kowalski, D. Cappelli, A. Moore, T. Shimeall, and S. Rogers, *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, Pittsburgh, Pa.: Carnegie Mellon Software Engineering Institute, 2005.

⁴ DHS, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*, Washington, D.C., 2009.

⁵ Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, Washington, D.C.: White House, February 12, 2013; Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, Washington,

Physical Assets

Akhunzada, Adnan, Mehdi Sookhak, Nor Badrul Anuar, and Abdullah Gani, "Man-at-the-End Attacks: Analysis, Taxonomy, Human Aspects, Motivation and Future Directions," *Journal of Network and Computer Applications*, Vol. 48, 2015, pp. 44–57.

https://www.researchgate.net/publication/278730778_Man-At-The-End_Attacks

This article discusses analytical problems associated with Man-at-the-End (MATE) models, because they do not incorporate granular human motivations or ability to be creative, attackers are construed to have unimpeded access to targets, and barriers to target access are effective only for a finite amount of time. The article concludes that future MATE modeling would improve through the incorporation of less technical frameworks and instead bring more human elements into projecting MATE end states.

Baracaldo, Nathalie, and James Joshi, "An Adaptive Risk Management and Access Control Framework to Mitigate Insider Threats," *Computers and Security*, Vol. 39, 2013, pp. 237–254.

<https://dl.acm.org/citation.cfm?id=2622880>

This article maintains that organization must find a balance between user-accessible features and the preservation of security controls to decrease overall systems risk. The researchers develop a framework according to the Role-Based Access Control model that incorporates a risk assessment processes with "the trust the system has on its users." The article finds that the model is useful in this context because it is able to detect anomalies and automatically remove system privileges when system trust falls below a set level. Findings include a proposed method for system administrators to incorporate inference modeling to achieve set levels and manage insider threats.

Keegan, Michael J., "Assessing Risk," in Mark A. Abramson, Daniel J. Chenok, and John M. Kamensky, eds., *Government for the Future: Reflection and Vision for Tomorrow's Leaders*, Lanham, Md.: Rowman & Littlefield Publishers and IBM Center for the Business of Government, 2018.

<http://www.businessofgovernment.org/sites/default/files/Chapter%20Seven%20Assessing%20Risk.pdf>

This chapter from a book by the IBM Center for the Business of Government describes various unique technological risks that government departments and agencies face before providing a series of recommendations. The publication discusses the use of blockchain technology, artificial intelligence, robotics, and other "smart" technologies that enable government productivity but offer new avenues for increased risk—e.g., the data that agencies share to achieve "interconnectedness" could open a means for attack.

The publication argues that legacy enterprise risk management governance mandated by OMB does not fully address the emerging state of technology and will need to incorporate changes, including how to prioritize and respond to unknowable risks.

Office of the Inspector General, U.S. Department of Defense, “U.S. European Command Needs to Improve Oversight of the Golden Sentry Program,” Washington, D.C., redacted, DODIG-2017-056, February 17, 2017.

<http://www.dodig.mil/reports.html/Article/1119358/us-european-command-needs-to-improve-oversight-of-the-golden-sentry-program-red/>

This (redacted) Office of the Inspector General report offers insight on U.S. European Command’s (EUCOM’s) Golden Sentry Program, a program that monitors the transfer of “defense articles and services provided to foreign governments or international organizations” through Foreign Military Sales as part of the Defense Security Cooperation Agency (DSCA) mission. The Office of the Inspector General chose four countries within EUCOM’s area of operations to determine whether DSCA’s end-use monitoring of transfers effectively prevented misuse or mishandling of materials. The report found that two of the four countries did not perform adequate oversight of activities that included the transfer of Javelin missiles and night-vision devices. The publication recommends that the both EUCOM’s Policy, Strategy, Partnering and Capabilities (J5/8) and DSCA’s Security Assistance and Equipping Directorate update outdated security checklists and validate receipt by foreign government purchasers.

Suh, Young A., and Man-Sung Yim, “‘High Risk Non-Initiating Insider’ Identification Based on EEG Analysis for Enhancing Nuclear Security,” *Annals of Nuclear Energy*, Vol. 113, 2018, pp. 308–318.

<https://www.sciencedirect.com/journal/annals-of-nuclear-energy/vol/113/suppl/C>

This recent research suggests the possibility of analyzing electroencephalography (EEG) signals to detect potential insider threats within nuclear-controlled facilities. The article draws on the observation of 11 individuals and their associated brain-wave activity in response to a series of questions. The researchers found significant brain-responses depending on the questions asked, particularly the “ β/α and γ/α ” wavelengths. The research suggest that use of EEG can increase the possibility of identifying “high-risk” insiders.

Information and Intellectual Property

Bailey, Christopher E., "Reform of the Intelligence Community Prepublication Review Process: Balancing First Amendment Rights and National Security Interests," *National Security Law Journal*, Vol. 5, 2017, pp. 203–237.
<https://www.nslj.org/wp-content/uploads/Bailey-Article-from-Vol.-5-Issue-2-complete-issue.pdf>

This article from George Mason University's *National Security Law Journal* traces the history of the prepublication process for previous members of the intelligence community and offers suggestions about how to mitigate U.S. national security risks that could occur in such publications. The article suggests that the Director of National Intelligence (DNI) should reexamine the "prepublication review process used by various intelligence agencies," which would help "advance U.S. national security while also ensuring minimal impairment of the First Amendment rights of government employees, military personnel, and contractors." The author states that the DNI can "remedy some of the current problems of overbroad and inconsistent regulations through clear regulatory guidance that helps management officials and employees alike meet both fiduciary and ethical obligations when it comes to protecting classified information."

Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, Washington, D.C.: White House, October 7, 2011.
<https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net>

This foundational executive order from the Obama administration calls for "responsible sharing and safeguarding of classified information on computer networks," that shall be "consistent with appropriate protections for privacy and civil liberties." Such structural reforms are intended to "ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government." The executive order policy applies to all agencies that "operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate, or access classified computer networks controlled by the [U.S. government]), and all classified information on those networks."

Holland, Rick, Rafael Amado, and Michael Marriott, *Too Much Information; Misconfigured FTP, SMB, Rsync, and S3 Buckets Exposing 1.5 Billion Files*, London: Digital Shadows, 2018.

<https://info.digitalshadows.com/rs/457-XEY-671/images/DigitalShadows-Research-DataExposure.pdf>

Research from Digital Shadows found more than 12,000 terabytes of sensitive information across several misconfigured websites. Researchers found that, although this was an international issue, U.S. website architectures provided the majority of publicly available sensitive information—especially those who use Amazon S3 buckets, Server Message Block, rsync, and file transfer protocols. The researchers found that third parties and other contractors composed the greatest risk of sensitive-data exposure.

Smith, Chelsea C., “Hacking Federal Cybersecurity Legislation: Reforming Legislation to Promote the Effective Security of Federal Information Systems,” *National Security Law Journal*, Vol. 4, No. 2, 2015, pp. 345–383.

https://www.nslj.org/wp-content/uploads/4_NatlSecLJ_345-385_Smith.pdf

This article examines the state of U.S. cybersecurity policy and related federal information system frameworks against the backdrop of the OPM data breach. The article states that, although some “limited regulatory legislation exists, the government lacks an enforcement mechanism to ensure federal agency compliance with statutory cybersecurity requirements.” The article outlines possible solutions for enforcement mechanisms and compliance metrics that could reduce risk to such future information systems.

Smith, Chelsea, Alexandra Diaz, and Richard Sterns, “Data Breach at a University: Preparing Our Networks,” *National Security Law Journal*, Vol. 5, No. 1, 2016, pp. 120–125.

https://www.nslj.org/wp-content/uploads/Spring-Symposium_Final_Website_2017-06-18.pdf

This article is a result of a symposium hosted by George Mason University’s Antonin Scalia Law School, the Law and Economics Center, and the *National Security Law Journal*. The symposium’s tabletop exercise focused on a hypothetical cybersecurity breach at a university and included 45 participants across the federal service. The tabletop exercise had two goals: (1) to develop a greater understanding of the various actors at play regarding the occurrence of a significant cyber incident and (2) to provide federal government attorneys greater knowledge of agency data-breach protocols.

U.S. Government Accountability Office, *Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risks*, Washington, D.C., GAO-04-678, May 2004.

<https://www.gao.gov/products/GAO-04-678>

This 2004 report from GAO notes the increasing reliance on contractors and subcontracts to develop software and other information systems for sensitive weapon capabilities and the associated supply chain risks. The report finds that DoD software acquisition policy does not address the risk imposed by foreign software developers, nor does the policy require the identification of potential risks by using certain foreign suppliers. Rather, most of the risks identified related to programmatic costs and schedules. Since DoD has neither the time nor the budget to test all “lines of code” to deliver to acquisition managers, GAO suggests that more preliminary research must be conducted to understand the contractors that the government chooses to work with.

U.S. Government Accountability Office, *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*, Washington, D.C., GAO-17-614, August 3, 2017.

<https://www.gao.gov/products/GAO-17-614>

This GAO report examines the steps that OPM has taken to mitigate the effect of the 2015 data breach and other preventive steps taken by the agency to protect against future attacks. GAO finds that OPM had made progress (various breakdown included within the report) with implementing the 19 recommendations mandated by DHS’s Computer Emergency Readiness Team but did not “consistently update completion dates for outstanding recommendations and did not validate corrective actions taken to ensure that the actions effectively addressed the recommendations.” Two other areas of concerns are a lack of oversight for continued use of contractor-operated systems and remaining unencrypted data on one high-value asset system.

U.S. Government Accountability Office, *Protecting Classified Information: Defense Security Service Should Address Challenges as New Approach Is Piloted*, Washington, D.C., GAO-18-407, 2018.

<https://www.gao.gov/products/GAO-18-407>

This GAO report follows up on a 2005 report examining the Defense Security Service’s (DSS’s) administration of the National Industrial Security Program.⁶ The report finds that, although DSS had “streamlined facility clearance and monitoring processes” and “strengthened the process for identifying contractors with potential foreign influence,” the organization faced resource constraints that prevented it from maintaining the workload and training needed to evolve with emerging threats and technology. For example, DSS was not able to conduct 60 percent of its security reviews at cleared

⁶ GAO, *Industrial Security: DOD Cannot Ensure Its Oversight of Contractors Under Foreign Influence Is Sufficient*, Washington, D.C., GAO-05-681, July 15, 2005.

facilities in FY 2016. DSS also continues to struggle with stakeholder information exchange, including government contractors and others within the intelligence community that address foreign intelligence threats. GAO recommends that DSS prioritize collaboration with stakeholders as the agency works to implement a new “monitoring system.”

Willison, Robert, Merrill Warkentin, and Allen C. Johnston, “Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives,” *Information Systems Journal*, Vol. 28, No. 2, 2018, pp. 266–293. <https://onlinelibrary.wiley.com/doi/abs/10.1111/isj.12129>

This article conducts a literature review to examine evidence regarding employee motivations to abuse computer privileges in the workplace. The researchers then apply a multitheoretical model as a way to explain such intentions. This model applies additional factors to the analysis through the incorporation of organizational justice (or perceived unfairness in the workplace) and certain facets of deterrence theory to better understand how policies affect individuals. The research findings suggest that individual employees may “form intentions to commit computer abuse if they perceive the presence of procedural injustice” and that “techniques of neutralization and certainty of sanctions moderate this influence” to some degree.

Organizational Resiliency and Risk Assessment

Literature is sparse on the nexus between personnel vetting and the ability of an organization to remain resilient in the face of adversity. Although there is a wide body of research focused on how organizations can remain competitive on a global scale, respond to economic shocks, and maintain branding (positive image), little exists on how the use of personnel vetting might increase organizational resilience.

This chapter includes a limited selection of baseline reference materials for developing measures of organizational resilience and highlights studies that reveal when personnel vetting considerations may affect resiliency efforts across different institutions. The ability of an organization to maintain operations in response to internal and external shocks (e.g., economic, natural disasters, or insider threat attacks) through careful planning and implementation of resilience measures can greatly assist in the mitigation of various risks to national security. The two main instruments of U.S. resilience policy are contained in Executive Order 13636 and Presidential Policy Directive 21.¹ The literature below also addresses the importance of maintaining strong avenues of communication with leadership to report on instances of organizational disloyalty and resource abuse.

Brooks, David, Jeff Corkill, Julie-Ann Pooley, Lynne Cohen, Cath Ferguson, and Craig Harmes, "National Security: A Propositional Study to Develop Resilience Indicators as an Aid to Personnel Vetting," *Proceedings of the 3rd Australian Security and Intelligence Conference*, 2010.

<https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1003&context=asi>

This paper examines the formulation of the Lifespan Resilience Scale, which attempts to measure individual resilience markers to aid national security vetting agencies as a proactive intervention tool. Although the tool is in the validation stage (controlled experiments with university students), the document suggests that this tool can assist in understanding whether particular individual attributes, family aspects, and other social environment interactions can serve as a measure of individual resilience in the face of adversity.

¹ Executive Order 13636, 2013; Presidential Policy Directive 21, 2013.

Hosseini, Seyedmohsen, Kash Barker, and Jose E. Ramirez-Marquez, "A Review of Definitions and Measures of System Resilience," *Reliability Engineering and System Safety*, Vol. 145, 2016, pp. 47–61.

<https://www.sciencedirect.com/science/article/pii/S0951832015002483>

This article reviews various organizational system modeling and evaluative measures for resilience. This article also provides an overview of the literature on system resilience (with an extensive focus on engineering systems), reviews gaps and emerging trends, and provides courses for further study.

Lee, Hun Whee, Jin Nam Choi, and Seongsu Kim, "Does Gender Diversity Help Teams Constructively Manage Status Conflict? An Evolutionary Perspective of Status Conflict, Team Psychological Safety, and Team Creativity," *Organizational Behavior and Human Decision Processes*, Vol. 144, 2018, pp. 187–199.

<https://www.sciencedirect.com/science/article/pii/S0749597816302205>

This article explores how status conflict ("disputes over the relative status positions of people in the social hierarchy of their group") can affect team psychological safety and team creativity. The authors find that such conflict can damage team creativity by "spawning a psychologically unsafe environment," but also that the "gender composition of a team seemed to help mitigate such detrimental consequences of status conflicts."

Linkov, Igor, Sabrina Larkin, and James H. Lambert, "Concepts and Approaches to Resilience in a Variety of Governance and Regulatory Domains," *Environment Systems and Decisions*, Vol. 35, No. 2, 2015, pp. 183–184.

<https://link.springer.com/article/10.1007/s10669-015-9553-6>

This article uses President Barack Obama's 2013 issuance of Executive Order 13636 and Presidential Policy Directive 21 to draw important distinctions between how to quantify resilience and how best to manage the application of resilience among U.S. government departments and agencies. The authors find that, although multiple U.S. government entities have attempted to "formalize" resilience within their respective mission spaces, efforts remain "fragmented and divergent." The article suggests that interagency collaboration to develop a more-institutionalized management system would begin to address some of the challenges currently faced. This article also agrees that a socioecological system-based approach is well suited for government resilience and should be combined with factors included within a proposed military installation resilience assessment that the authors recommend be implemented.

Marlow, Shannon L., Christina N. Lacerenza, Jensine Paoletti, C. Shawn Burke, and Eduardo Salas, "Does Team Communication Represent a One-Size-Fits-All Approach? A Meta-Analysis of Team Communication and Performance," *Organizational Behavior and Human Decision Processes*, Vol. 144, 2018, pp. 145–170.

<https://www.sciencedirect.com/science/article/pii/S074959781630125X>

This article examines the impact of team communication on organizational performance. It particularly seeks to present a framework for understanding various characteristics of team communication, performance, and relationships with organizational performance. The research team argues that distinguishing between "different communication types in both practical and theoretical applications" can enable organizations to better understand their workforce.

Rowe, Mary, "Fostering Constructive Action by Peers and Bystanders in Organizations and Communities," *Negotiation Journal*, Vol. 34, No. 2, 2018, pp. 137–163.

<https://onlinelibrary.wiley.com/doi/abs/10.1111/nejo.12221>

This article argues that peers and bystanders can play an important role in organizational conflict. The author states that bystanders can assist with three functions of a conflict management system, by identifying, assessing, and managing behaviors that the "organization or community deems to be unacceptable." Rowe uses experience drawn from 45 years of organizational study to draw relevant examples of how bystanders can play important roles in reducing safety violations, fraud, theft, national security violations, and cybersabotage.

Sikula, Nicole R., James W. Mancillas, Igor Linkov, and John A. McDonagh, "Risk Management Is Not Enough: A Conceptual Model for Resilience and Adaptation-Based Vulnerability Assessments," *Environment Systems and Decisions*, Vol. 35, No. 2, 2015, pp. 219–228.

<https://link.springer.com/article/10.1007/s10669-015-9552-7>

This article contends that traditional U.S. risk-based methods of protecting critical infrastructure are limited because they "rely upon foreseeable factor analyses of steady-state systems with predictable hazard frequencies and severities." Further, there has been an overemphasis on the study and application of engineering resilience approaches that cannot account for current capabilities in "complex adaptive systems." Rather, the article indicates that an amalgamation of legacy risk approaches should be combined with socioecological resilience principles that could improve federal agencies' understanding to manage and assess unforeseeable events.²

² For more research related to the socioecological method, see L.V. Astakhova, "Evaluation Assurance Levels for Human Resource Security of an Information System," *Procedia Engineering*, Vol. 129, 2015; and Jeffrey Hunker and Christian W. Probst, "Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, Vol. 2, No. 1, 2011.

Fraud Detection

The literature related to the gaming industry (e.g., casinos) offers relevant vetting insights through the use of technology to detect insider fraud on gambling floors, which many times can cost casino business owners thousands of dollars in seconds if not addressed in a timely manner. The literature suggests that insider threats within the casino industry use many of the same methods (e.g., small portable devices) in an attempt to exfiltrate high-value items. For an insider threat within a technology firm, this may take the form of a mobile USB device; for an insider threat within a casino, it could simply mean attempts to grab chips from a table. Tracking large volumes of cash or casino chips across employees and patrons is comparable to the difficulty in monitoring web traffic and data downloads for an organization. Casino fraud detection also uses similar tools and techniques found in other categories of vetting concerns, such as insider threats and continuous monitoring. Casinos incorporate such technologies as optical variable technology within card decks and chips sets that can signal to dealers and floor managers whether devices may be in use to commit fraud. The use of such technologies within a vetting context could aid visual security feeds to ensure that only department- or agency-approved materials enter sensitive locations. The literature also offers other techniques currently in development to combat fraudulent practices for online casinos. The large number of users, coupled with increased access points, allows a large amount of financial transactions requiring different methods and software to detect and deter fraud.

This chapter includes selected literature on fraud detection best practices in the banking and gaming industries. Examining fraud prevention across these two industries has important implications for personnel vetting practices. For example, fraudulent practices mean different things to different organizations; for DoD, they could mean wasted resources; for the Department of Justice or the Department of the Treasury, fraud could translate into economic abuse, such as white-collar crime; for the banking industry, fraud could mean the detection of false identities to gain access to checking accounts. Ensuring adequate fraud protection is important for the private sector, and fraud detection considerations may be especially important now given the breadth of personal data acquired during the 2015 OPM data breach.

Baysden, Chris, "What You Can Learn About Fraud Prevention from a Casino: An Internal Auditor at Caesars Palace Shares the House's Tips for Detecting and Combating Fraud," American Institute of Certified Public Accountants, May 21, 2014.

https://www.aicpastore.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2014/FVSNews/fromacasino.jsp

This short article from the American Institute of Certified Public Accountants presents a view of casino fraud from an internal auditor at Caesars Palace in Las Vegas. The auditor explains that the majority of fraud cases that he has seen occurs not on the floor of the casino but rather in the hospitality and retail sections of gaming venues. The article presents best practices for casinos, including making better use of the data generated while individuals are working on the premises, increasing the expertise of surveillance personnel through training, and continually evaluating access control measures.

Bunn, Matthew G., and Kathryn M. Glynn, "Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries," *Journal of Nuclear Materials Management*, Vol. 41, No. 3, pp. 4–16.

https://dash.harvard.edu/bitstream/handle/1/10861136/Preventing%20Insider%20Theft-V%2041_3.pdf

This journal article uses a series of private-industry interviews and a literature review of security practices in Las Vegas casinos and the pharmacy industry to develop preventive security measures for controlling nuclear industry materials. The researchers find that uninterrupted video surveillance, well-maintained security logs, two-person oversight of products (using individuals who have separate reporting chains and who do not usually interact), and splitting personnel responsibilities between security and surveillance can greatly contribute to material accountability.

Casinos Security, "Anti-Fraud Detection System," webpage, undated.

<http://casinossecurity.com/anti-fraud-detection.htm>

This webpage points to the emerging abuse (and fraudulent detection) of online casinos. The large number of users, coupled with increased access points, allows a large amount of financial transactions requiring different methods and software to detect and deter fraud. Whereas traditional casinos have increasingly relied on different methods of credentialing—including the use of hotel key verification and cashless machine cards (cards that retain the balance of winnings)—online casinos must approach the problem differently. Some casinos have partnered with such companies as Ethoca, which helps monitor user activity. Online casinos are also beginning to partner with secure online banking sites, such as Eproc and DataCash, which provide an additional layer of security for financial transactions. Online casinos also must operate on the latest software to avoid potential financial hackers and have partnered with Playtech, Microgaming, and Cryptologic to ensure player anonymity and site protection.

Committee of Sponsoring Organizations of the Treadway Commission, *Fraud Risk Management Guide: Executive Summary*, New York, September 2016.

<https://www.coso.org/Documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf>

This publication offers a guide to fraud risk management that draws on best practices gained from a 2008 product (*Managing the Business Risk of Fraud: A Practical Guide*) published by the American Institute of CPAs, the Institute of Internal Auditors (IIA), and the Association of Certified Fraud Examiners (ACFE). This publication updated the former, adding in new inputs to account for the emergence of new technology to detect fraudulent activities, such as the use of data analytics. The framework contained within this document also uses 17 “internal control principles” formerly adopted for use by the Standards for Internal Controls issued by the comptroller general.

Efanov, Dmitry, and Pavel Roschin, “The All-Pervasiveness of the Blockchain Technology,” *Procedia Computer Science*, Vol. 123, 2018, pp. 116–121.

<https://www.sciencedirect.com/science/article/pii/S1877050918300206>

This article outlines uses of blockchain technology (“a distributed database containing records of transactions that are shared among participating members”) to combat fraud in the workplace. Blockchain technology ensures that all transaction conform to the “consensus of a majority of the members,” making “fraudulent transactions unable to pass collective confirmation.” The article concludes with some perspective on using blockchain to combat future instances of fraud across a variety of settings.

FICO, “5 Keys to Successfully Applying Machine Learning and AI in Enterprise Fraud Detection,” white paper, San Jose, Calif., July 2018.

<https://www.fico.com/en/resource-download-file/4540>

This white paper from FICO explores uses of machine learning algorithms to detect fraudulent behavior in the workplace. The article suggests that machine learning systems should be incorporated into organizations as soon as possible, not only to detect current fraudulent activities but also to help build baseline to detect future anomalies. FICO explains that there are seven different kinds of profiles that can be used to detect fraud and develop the appropriate machine learning program: (1) transaction profiles (for consumers’ financial and nonfinancial activity), (2) collaborative profiles (which identify behaviors that differ from typical behavior), (3) behavior sorted lists (which rank recurrent activities that are unique to individuals), (4) merchant profiles (aggregated scores to provide strategic view of risk), (5) multilayered self-calibrating profiles (which detect outliers if data to train program are nonexistent), (6) user-defined profiles (custom designed for specific devices or IPs), and (7) global intelligent profiles (real-time adaptive risk rankings to flag files for fraud assessment).

Jonas, Jeff, "Threat and Fraud Intelligence, Las Vegas Style," *IEEE Security and Privacy*, Vol. 4, No. 6, 2006.

<https://jeffjonas.typepad.com/IEEE.Identity.resolution.pdf>

This article examines the efficiency and effectiveness of using identity resolution to detect and deter fraud within the casino industry. The author (an IBM researcher) discusses the three most prevalent types of matching systems and methods currently in use by casinos (and others within advertising): (1) the "merge/purge and match/merge" method, which ingests data and eliminates duplicate records; (2) the "binary" matching engine, which tests one identity in one data set for its presence in a second data set; and (3) the use of "centralized identity catalogues," which collect identity data from both "disparate and heterogeneous data sources" to create one unique identity. The article indicates that industries must strive to achieve "real time awareness" of personal identities, given the proliferation and ease for individual to create false identities.

Kelly, Christopher, and Frans Deklepper, "On the Hunt for Payroll Fraud: Taking a Close Look at Payroll Risks Can Enable Internal Auditors to Help Their Organizations Save Money and Identify Wrongdoing," *Internal Auditor*, Vol. 73, No. 2, 2016, pp. 45–51.

<http://go.galegroup.com/ps/anonymous?id=GALE%7CA450695662&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00205745&p=AONE&sw=w>

This article explores various shift differences (full time, hourly, night shift, mobile, and telework) that can pose different categories of economic risk to organizations. Such risks include false claims for allowances, overpayment for weekends and holidays, and even salaries to employees who have left the organization. The article suggests that the use of database monitoring can greatly enhance the prevention of fraudulent activities and can track malign employee behavior that often goes unreported. The article also suggests that human resources departments might be able to assist in creating the baseline for databases, since they track overtime pay, which employees gained most frequently from weekend and public holiday pay, and other entry and exit badge data needed to calculate time spent in the office.

Kelly, Patrick, and Carol A. Hartley, "Casino Gambling and Workplace Fraud: A Cautionary Tale for Managers," *Management Research Review*, Vol. 33, No. 3, 2010, pp. 224–239.

<https://www.emeraldinsight.com/doi/abs/10.1108/01409171011030381>

This article examines cases of casino fraud found within the state of Connecticut. The authors find that the risk of financial fraud can be linked to the growing problem of gambling addiction—at least in the region studied—further suggesting that employees who live within 50 miles of casino are more likely to develop such addictions that can present increased risk to their employers. The article then lays out recommendations for organization managers living within this radius, including increased use of

internal audit procedure, increased manager review of “key business documents,” and improved controls of cash receipts and check registers.

West, Jarrod, Maumita Bhattacharya, and Rafiqul Islam, “Intelligent Financial Fraud Detection Practices: An Investigation,” paper presented at the International Conference on Security and Privacy in Communication Networks, Beijing, September 2014.

<https://arxiv.org/pdf/1510.07165.pdf>

This paper discusses the increased risk for fraud as companies move their organizational finances to cloud and other mobile computing platforms. The authors explain that traditional mechanisms to detect fraud, such as manual observation or intermittent auditing, will be unable to thwart new avenues for fraud, given the increasing use of such systems. The paper uses a series of case studies to determine whether new fraudulent detection mechanisms, such as data mining and other computational intelligence program, can assist in the prevention of financial fraud.

Credentialing

U.S. departments and agencies draw credentialing standards from different documents, depending on required access and missions. For DoD and the service components, Common Access Card (CAC) managers draw guidance from three documents: (1) DoD Instruction 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*; (2) DoD Manual 1000.13, Vol. 1, *DoD Identification (ID) Cards: ID Card Life-Cycle*; and (3) DoD Manual 1000.13, Vol. 2, *DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*.¹ Homeland Security Presidential Directive 12 provides policy for creating a common identification system for federal employees and contractors and mandates the development and implementation of a government-wide standard for secure and reliable forms of identification issued by the U.S. government to its employees and contractors.² Other agencies outside DoD rely on separate National Institute of Standards and Technology Federal Information Processing Standards for the issuance of Personal Identity Verification needed to access sensitive information systems. The Transportation Worker Identification Credential (TWIC) became public law under the Maritime Transportation Security Act of 2002, which is required for civilian workers needing access to secure areas of the nation's maritime facilities and vessels.³ There has also been case law related to credentialing.⁴

¹ DoD Instruction 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, Washington, D.C.: U.S. Department of Defense, January 23, 2014, incorporating change 1, December 14, 2017; DoD Manual 1000.13, *DoD Identification (ID) Cards: ID Card Life-Cycle*, Vol. 1, Washington, D.C.: U.S. Department of Defense, January 23, 2014; DoD Manual 1000.13, Vol. 2, *DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, Vol. 2, Washington, D.C.: U.S. Department of Defense, January 23, 2014.

² Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, Washington, D.C.: U.S. Department of Homeland Security, August 27, 2014.

³ Pub. L. 107-295, Maritime Transportation Security Act of 2002, Section 102, November 25, 2002.

⁴ At least one major challenge to the use of credentialing was contented in the case of *NASA v. Nelson*, 562 U.S. 134, 2011. In this case, a government contractor challenged the use of background investigations to acquire his government credentials, believing that the investigation required was unreasonably intrusive. The case was a

This chapter includes selected literature regarding U.S. policies governing employee credentials (e.g., badges and identification cards) and related barriers that organizations have faced in implementing such policies. Because a substantial part of personnel vetting relates to the types of accesses an individual will gain once adjudicated, understanding baseline policies for different credentialing program are vital.

Office of Personnel Management, “Memorandum for Heads of Departments and Agencies, Chief Human Capital Officers, and Agency Security Officers: Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide,” Washington, D.C., January 14, 2008.

<https://www.opm.gov/suitability/suitability-executive-agent/policy/decision-making-guide.pdf>

This memorandum serves as an excellent reference for the credentialing process and outlines authorities agencies can use to “act” on “unfavorable information” found through the course of associated background investigations and contains adjudicative criteria “decision points” (e.g., does the conduct and character of the competitive service or career Senior Executive Service applicant, appointee, or employee promote the efficiency or protect the integrity of the competitive service?) for credentialing decisions, including applicable authorities, Code of Federal Regulations, or Merit Systems Protection Board processes. This reference also provides credentialing (Homeland Security Presidential Directive 12⁵) guidance, policy references, and specific adjudicative criteria at certain “decision points” within the Security, Suitability, and Credentialing timeline. This reference also clarifies the “scope of the various authorities agencies may currently utilize to act on unfavorable information.”

Office of the Inspector General, U.S. Department of Defense, *Followup Audit: Navy Access Control Still Needs Improvement*, redacted version, Washington, D.C., DODIG-2016-018, November 9, 2015.

<https://www.dodig.mil/reports.html/Article/1119227/followup-audit-navy-access-control-still-needs-improvement-redacted/>

This report depicts information, in redacted form, that highlights the continued issues that service components face when credentialing personnel who require base access. The report specifically sought to determine whether Navy installations were able to obtain access to the National Crime Information Center (NCIC) or various “Terrorist Screening databases” to conduct “checks of contractor personnel enrolled in the Navy Commercial Access Control System” before credentialing issuance, as well as whether the use of such databases addressed problems noted in the full report. The report finds that although “vetting capability,” such as access to databases (NCIC, Triple-I,

direct challenge to Homeland Security Presidential Directive 12 (2014), although the Supreme Court held that investigation required for the credential did not violate any Civil Service Reform Act protections.

⁵ Homeland Security Presidential Directive 12, 2014.

and OpenFox), were supplied to installation security personnel, the queries used did not return information that otherwise would have precluded certain personnel from accessing the bases.

Office of the Inspector General, U.S. Department of Defense, *DoD Needs to Improve Screening and Access Controls for General Public Tenants Leasing Housing on Military Installations*, Washington, D.C., DODIG-2016-072, April 1, 2016.

<https://media.defense.gov/2016/Sep/22/2001774203/-1/-1/1/DODIG-2016-072.pdf>

This report, made available to the public, explores the difficulty in obtaining adequate security controls to ensure that effective measures are in place during the DoD Military Housing Privatization Initiative. The Office of the Inspector General found three instances when DoD security officials did not “effectively screen” or provide “adequate control installation access for general public tenants who leased privatized housing.” The report notes that Army and Air Force guidance for Fort Detrick, Naval Station Mayport, and Barksdale Air Force Base had not defined a process to “obtain background checks or require that badge expiration dates align with lease terms,” nor maintained associated screening systems used to conduct background checks on tenants. The Office of the Inspector General recommends that the service components update guidance to reflect National Crime Information Center and Interstate Identification Index file requirements for base housing access and conduct a full review of base-housing credentials across other bases with the Military Housing Privatization Initiative to minimize risk.

Office of the Inspector General, U.S. Department of Homeland Security, *TWIC Background Checks Are Not as Reliable as They Could Be*, Washington, D.C., OIG-16-128, September 1, 2016.

<https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-128-Sep16.pdf>

This report examines the issuance of TWIC by TSA to individuals requiring unescorted access through secure maritime and shipping facilities. The Office of the Inspector General found that a lack of TWIC program oversight hampered overall program effectiveness, specifically within the security threat assessment (background check) process: (1) Fraud detection techniques are not monitored and not used in completing the background checks, (2) adjudicators may grant TWICs even if questionable circumstances exist, (3) quality assurance and internal control procedures are missing from the background check and terrorism vetting processes, and (4) efforts tested for continuous vetting for disqualifying criminal or immigration offenses lack measures to determine the best solutions. According to the Office of the Inspector General, the TWIC program office lacks visibility and authority over TSA, which has manifested in several risks to issued credentials. The Office of the Inspector General rec-

ommended that involved stakeholders establish a cross-function coordinating entity to provide regular oversight of TWIC programs and procedures.⁶

Office of the Inspector General, U.S. Department of Homeland Security, *Review of Coast Guard's Oversight of the TWIC Program*, Washington, D.C., OIG-18-88, September 28, 2018.

<https://www.oig.dhs.gov/sites/default/files/assets/2018-10/OIG-18-88-Sep18.pdf>

This report continues the discussion of TWIC program implementation under DHS and the challenges the U.S. Coast Guard has faced because of a lack of guidance. Several factors complicated the universal use of TWIC by DHS to protect ports of entry between FY 2016 and FY 2017: (1) DHS faced challenges in identifying the responsible TWIC office to conduct oversight, (2) the Coast Guard was still working to create a list of facilities that posed greater risk (“dangerous cargo”), and (3) the Coast Guard used “electronic readers” an average of one in every fifteen TWIC cards against TSA’s canceled TWIC accesses. The Office of the Inspector General noted that this lapse is likely a result of failing card readers scattered across operating locations.

U.S. Government Accountability Office, *VA Health Care: Improved Oversight and Compliance Needed for Physician Credentialing and Privileging Processes*, Washington, D.C., GAO-10-26, January 6, 2010.

<https://www.gao.gov/products/GAO-10-26>

This GAO report traces the VA’s use of physician credentialing, as required by agency policy. In 2008, nine patients were found to have died from poorly conducted surgeries and poor postsurgical care. The report specifically follows up on noted credentialing issues at the Marion, Illinois, VA Medical Center (VAMC) and also conducted a sampling of policy requirements at similar VA locations. The report finds that, although other locations had not experienced the extent of issues witnessed in Marion, VAMCs collectively did not follow the credentialing policy instituted by the VA. For example, GAO finds that 29 out of 180 credentialing and privileging files reviewed “lacked proper verification of state medical licensure” and did not attempt to investigate “omitted required information on their application,” and there were another 21 cases where “malpractice information was not disclosed” by physicians. GAO was able to uncover much of the missing malpractice information in publicly available databases.⁷

⁶ See also U.S. Government Accountability Office, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, Washington, D.C., GAO-05-106, December 10, 2004.

⁷ See also U.S. Government Accountability Office, *VA Health Care: Improved Screening of Practitioners Would Reduce Risk to Veterans*, Washington, D.C., GAO-04-566, March 31, 2004; and J. B. FitzHarris, I. Jacoby, S. B. Permison, and P. McCardle, “Challenges of Including Dietitians, Nurses, Occupational Therapists, and Pharmacists in the Federal Credentialing Program,” *Military Medicine*, Vol. 165, No. 10, 2000.

U.S. Government Accountability Office, *Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards*, Washington, D.C., GAO-11-751, September 20, 2011.

<https://www.gao.gov/products/GAO-11-751>

This GAO report provides an assessment of whether federal agencies have adhered to the guidance and direction provided in Homeland Security Presidential Directive 12,⁸ National Institute of Standards and Technology documents, and OMB standards and guidance and identifies obstacles agencies have faced during implementation processes. The report finds that the Departments of Agriculture, Commerce, Homeland Security, Housing and Urban Development, Interior, and Labor and NASA and the Nuclear Regulatory Commission had made “mixed progress” in instituting directive’s standards. At a more granular level, they faced obstacles in creating Personal Identity Verification cards that could be accepted by multiple departments and agencies and issues with credentialing employees working off-site, and they often struggled with tracking (and revoking) issued credentials.⁹

U.S. Government Accountability Office, *Government Publishing Office: Production of Secure Credentials for the Department of State and U.S. Customs and Border Protection*, Washington, D.C., GAO-15-326R, March 10, 2015.

<https://www.gao.gov/products/GAO-15-326R>

This GAO report follows the decision by the Customs and Border Protection to choose the Government Publishing Office (GPO) as its primary vendor for secure credentials and the various reasons for doing so, including (1) GPO’s history of producing secure credentials for federal agencies, (2) GPO’s off-site backup production facilities, (3) the close working relationship between GPO and the Department of State as the official issuer of passports, and (4) GPO’s ability to provide a secure supply chain. GPO self-reports that its supply chain is secure, as it first procures the raw materials from the private sector (polymers, inks, and radio-frequency identification [RFID]) before final assembly at its production sites.¹⁰

⁸ Homeland Security Presidential Directive 12, 2014.

⁹ See also U.S. Government Accountability Office, *Employee Security: Implementation of Identification Cards and DoD’s Personnel Security Clearance Program Need Improvement*, Washington, D.C., GAO-08-551T, April 9, 2008.

¹⁰ Also see Office of Inspector General, Office of Audits, NASA, *Audit of NASA’s Information Technology Supply Chain Risk Management Efforts*, Washington, D.C., IG-18-019 (A-17-008-00), May 24, 2018; Office of the Inspector General, U.S. Department of Defense, *The Missile Defense Agency Can Improve Supply Chain Security for the Ground-Based Midcourse Defense System*, redacted version, Washington, D.C., DODIG-2017-076, April 27, 2017.

U.S. Government Accountability Office, *Military Personnel: Performance Measures Needed to Determine How Well DoD's Credentialing Program Helps Servicemembers*, Washington, D.C., GAO-17-133, October 17, 2016.

<https://www.gao.gov/products/GAO-17-133>

This report follows a credentialing identification program implemented by DoD to help service component personnel find equivalent civilian licenses and programs for end-of-service transitions. Although the focus of the GAO report is on establishing metrics of performance, the report highlights the successful implementation of the USA 4 Military Families program, which identifies “state-level professional requirements that can be met through the training received by servicemembers in the armed forces” and “strategies to remove barriers to servicemembers’ efforts to attain credentials.” This initial pilot program was implemented within six U.S. states and examines how the program was able to accelerate the hiring of service veterans for civilian positions through information sharing.

Information Sharing and Reciprocity

Information-sharing and reciprocity agreements between federal departments and agencies are fundamental to the personnel vetting process. Good information exchange can relay important facts to an investigator regarding an individual's particular history (e.g., criminal records, academic credentials, unexplained absences from military duties) and help cross-validate information gained during interviews. There are examples of a lack of information exchange inhibiting vetting processes, such as state laws that prevent the disclosure of expunged cases or combatant command military records for infractions that are not properly recorded or uploaded into databases. Reciprocity functions become important once employees are adjudicated, especially in instances when an individual might be negatively adjudicated for one agency (such as the FBI) but gain access to similar information through another agency (such as a contractor office).

This chapter includes selected literature regarding reciprocity and information-sharing agreements among U.S. government departments and agencies. Some of the literature notes the struggle to implement security clearance reciprocity among the executive branch and other instances of how information sharing is used to combat various threats.

Executive Order 12968, *Access to Classified Information*, Washington, D.C.: White House, August 2, 1995.

<https://fas.org/sgp/clinton/eo12968.html>

President Bill Clinton signed this executive order in August 1995 to provide “eligibility standards for agency heads in granting access to National Security Information.” The order provides further details on the investigative and adjudicative requirements for each level of security clearance access. This was a foundational document in this category, since it defined the specific conditions for when reciprocity applies to federal employees and the circumstances in which reciprocity could be denied.

Financial Action Task Force, *FATF Guidance: Private Sector Information Sharing*, Paris, November 2017.

<http://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf>

This report released by the intergovernmental Financial Action Task Force highlights the importance of information sharing to combat illicit financial flows and includes both global anti-money laundering (AML) and counterterrorist financing (CFT) standards. A critical part of information exchange for the includes international financial partners, which much of the black market or other illicit schemes emanate from. Main challenges to the AML and CFT campaigns are a result of insufficient information-sharing agreements between U.S. and international financial partners.

Intelligence and National Security Alliance, *Security Clearance Reciprocity: National Standards and Best Practices to Expedite Clearance Transfers*, Arlington, Va., July 2017.

<https://www.insaonline.org/wp-content/uploads/2017/07/INSA-Security-Clearance-Reciprocity-July-2017.pdf>

This document analyzes reciprocity processing timelines reported by contractors to show that the time required to transfer personnel clearances varies widely by agency—suggesting that some agencies’ business processes may be more efficient than others’. The document recommends that the Office of the Director of National Intelligence identify the factors that facilitate or impede efficient transfers of clearances and consider how the intelligence community (IC) can adopt agencies’ best practices as the foundation for reciprocity policy.

Intelligence Community Policy Guidance 704.4, *Reciprocity of Personnel Security Clearance and Access Determinations*, Technical Amendment, Washington, D.C.: Office of the Director of National Intelligence, June 20, 2018.

<https://www.dni.gov/files/documents/ICPG/cleanedICPG-704.4---Reciprocity-of-Personnel-Security-Clearance-and-Access-Determinations-6-Jun-2018.pdf>

This policy amends previous Intelligence Community Policy Guidance 704.4 on Sensitive Compartmented Information (SCI) reciprocity within the U.S. IC to include additional reciprocity information. IC agencies are instructed to accept Single Scope Background Investigation and polygraph examinations if conducted by another IC element, as long as such investigative procedures were conducted within the past six years; however, agencies can determine to accept this level of clearance at the seven-year mark, or older, on a case-by-case basis.

Platt, Jody E., Peter D. Jacobson, and Sharon L. R. Kardia, "Public Trust in Health Information Sharing: A Measure of System Trust," *Health Services Research*, Vol. 53, No. 2, 2018, pp. 824–845.

<https://onlinelibrary.wiley.com/doi/pdf/10.1111/1475-6773.12654>

This journal article measures levels of individual trust within a health system to try to predict four characteristics of organizational trust: competency, fidelity, integrity, and overall trustworthiness. The study used a sample size of 1,011 individuals to conduct a linear regression analysis with associated demographics and other psychosocial predictors. The study found that only 12.5 percent of the population sample "trusted" their particular health system, suggesting that organizations need to focus on "engendering public trust" to rebuild faith within the system.

Presidential Decision Directive/NSC-63, *Critical Infrastructure Protection*, Washington, D.C.: White House, May 22, 1998.

<https://fas.org/irp/offdocs/pdd/pdd-63.htm>

This directive describes risks associated with U.S. critical infrastructure and mandates the implementation of Information Sharing and Analysis Centers (ISACs) to address potential physical and cyber-based attacks that could affect important military or economic U.S. centers of gravity. The directive requires each of the federal government's 16 critical infrastructure sectors to establish ISACs that would act as information-sharing hubs between the public and private sectors. Later, in 2003, the National Council of ISACs was stood up to coordinate information exchange between the centers.

Public Law 108-458, *Terrorism Prevention Act of 2004*, December 17, 2004.

<https://www.govinfo.gov/content/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf>

Title III of the Intelligence Reform and Terrorism Prevention Act (Pub. L. 108-458) contained statutory guidelines for the reciprocity of security clearances. This public law updated the 1995 Executive Order 12968 reciprocity mandates for transference, where applicable, of security clearances among sponsoring government agencies.

Security Executive Agent Directive 7, *Reciprocity of Background Investigations and National Security Adjudications*, Washington, D.C.: Office of the Director of National Intelligence, November 9, 2018.

https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-7_BI_ReciprocityU.pdf

Security Executive Agent Directive (SEAD) 7 reaffirms the requirements for reciprocal acceptance of background investigations and national security adjudications for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. SEAD 7 defines reciprocity as the "acknowledgement and acceptance of an existing background investigation conducted by an authorized investigative agency; the acceptance of a national security eligibility adjudication determined by an autho-

alized adjudicative agency; and the acceptance of an active national security eligibility determination granted” by the executive branch.

U.S. Department of Homeland Security, *Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community*, Washington, D.C., October 2016.

<https://www.dhs.gov/publication/ci-threat-info-sharing-framework>

This DHS framework builds on previous ISAC considerations, serving as a baseline resource to assist in the creation of a federal, state, local, tribal, and territorial (SLTT) information-sharing mechanism. SLTTs are an important part of the DHS information-sharing mission, since their departments and agencies can often perceive and report threats long before they reach the federal level. Although this framework does not present particular policy changes, it presents results from the 2012 National Strategy for Information Sharing and Safeguarding and the DHS National Infrastructure Protection Plan regarding the desire to share “actionable and relevant information across the critical infrastructure community.”¹ This framework also describes all information-sharing processes currently in use with SLTTs and other federal partners and provides several case studies in which information exchange blunted attempts to undermine U.S. infrastructure.

U.S. Government Accountability Office, *Security Clearances: FBI Has Enhanced Its Process for State and Local Law Enforcement Officials*, Washington, D.C., GAO-04-596, April 30, 2004.

<https://www.gao.gov/products/gao-04-596>

This GAO report discusses the difficulties with information sharing between cleared and noncleared populations within the United States. For example, law enforcement officials are often expected to be at the forefront of combating terrorism yet usually do not make up part of the federally cleared community. The FBI has led the federal effort to clear law enforcement officials in the post-2001 era, though the process has created “frustration” within the law enforcement community, which can be a low priority for the bureau. This report traces the FBI’s process for clearing law enforcement personnel, with a particular focus on how the FBI has attempted to facilitate information exchange with state law enforcement.

¹ White House, *National Strategy for Information Sharing and Safeguarding*, Washington, D.C., 2012; DHS, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, Washington, D.C., 2013.

U.S. Government Accountability Office, *Transportation Security: DHS Efforts to Eliminate Redundant Background Check Investigations*, Washington, D.C., GAO-07-756, April 26, 2007.

<https://www.gao.gov/products/GAO-07-756>

This important study by GAO examined the similarities of six separate DHS background check programs: Hazardous Materials Endorsement, Transportation Worker Identification Credential, Merchant Mariner Document, Free and Secure Trade, Secure Identification Display Areas, and Air Cargo. The purpose of the study was to identify redundancies across these six vetting programs to see what types of investigations might be consolidated to reduce security check backlogs. GAO finds not only that similar background checks have a range of associated costs but also that there are major differences in reasons for denying credentials. GAO was ultimately unable to determine the extent of redundant background checks for DHS employees, because the department did not maintain records of the multiple checks.

Willis, Henry H., Genevieve Lester, and Gregory F. Treverton, "Information Sharing for Infrastructure Risk Management, Barriers and Solutions," *Intelligence and National Security*, Vol. 24, No. 3, June 2009.

https://create.usc.edu/sites/default/files/publications/informationsharingforinfrastructure-risk-management-barriers_0.pdf

This article from 2009 explains that, although infrastructure protection is "usually viewed as a public responsibility," infrastructure risk management "requires a high degree of cooperation between the public and private sectors, particularly in the sharing of information about risks to infrastructure." Researchers held discussions with several chief security officers across different sectors of the United States, which revealed the complex set of private-sector requirements. The researchers find that the United States had established "many mechanisms for sharing information," but remaining barriers can "inhibit both the private and public partners from obtaining the information needed to protect infrastructure."

Wood, Suzanne, and Lynn F. Fischer, *Cleared DoD Employees at Risk—Report 1: Policy Options for Removing Barriers to Seeking Help*, Monterey, Calif.: Defense Personnel and Security Research Center, MR 01-02, January 2002.

<https://www.dhra.mil/Portals/52/Documents/perserec/mr01-02.pdf>

This first report (in a two-part series) provides information on DoD-specific recommendations for how best to address personal struggles (e.g., relationship counseling, mental health issues) while also ensuring continued access to classified materials. The report notes that issues arise when employees might forgo professional psychological or emotional counseling out of a fear of losing their clearance. This report suggests that managers must ensure that federal employees are aware of the many protections afforded through the employee assistance program, since many fears of reprisals are often unfounded.

Wood, Suzanne, and Lynn F. Fischer, *Cleared DoD Employees at Risk—Report 2: A Study of Barriers to Seeking Help*, Monterey, Calif.: Defense Personnel and Security Research Center, TR 01-04, January 2002.

<https://www.dhra.mil/Portals/52/Documents/perserrec/tr01-04.pdf>

This second report (in a two-part series) on seeking professional help (in the context of maintaining a security clearance) explores the relationship between DoD security policies and federal employee assistance programs for both civilians and military service members. The report finds that, even though there are policies in place to protect individuals in such circumstances, fear of repercussions often forces employees to seek assistance outside the U.S. government.

Five Eyes Partner Practices

The U.S. Five Eyes (FVEY) partnership (a multilateral information sharing partnership) was established in the post–World War II era to increase information exchange between the United States, the United Kingdom, Canada, Australia, and New Zealand. The FVEY partnership enjoys greater exchanges of intelligence information, given the collective security posture and vision shared among the countries. This partnership differs from the scope of intelligence information shared within a NATO environment, where national security interests may differ among coalition partners, therefore posing different levels of sensitive information risks. Each of the FVEY nations has developed its own unique vetting processes that could help inform vetting options being considered for the United States.

This chapter includes selected literature regarding how U.S. FVEY partners conduct vetting, noting unique practices that may be relevant for U.S. policymakers to consider. Notably, RAND confirmed through an informal discussion with FVEY leadership that most of the vetting protocols in these countries are classified at the Secret level or higher, precluding references to such materials in a public document. This chapter also includes reference to selected FVEY government websites that can provide additional materials for gaining a better understanding of partner vetting practices.

United Kingdom

Overview

The United Kingdom Security Vetting (UKSV) was the sole provider of security clearances as of January 2017. In 2015, the United Kingdom’s Strategic Defence and Security Review consolidated all of the United Kingdom’s security vetting offices into the singular UKSV structure, with a mandate to (1) establish a single vetting database, (2) develop “portable vetting,” and (3) standardize the cost of clearance checks across government services.¹ This section notes the main locations for finding publicly avail-

¹ UK Ministry of Defence, “Guidance: United Kingdom Security Vetting,” webpage, last updated August 2, 2019. The UKSV brought together two previously separate entities, the Defence Business Services National Secu-

able information related to the UKSV's vetting process and other important strategic documents that guide the overall UK security clearance process. The United Kingdom requires individuals to enter the vetting process if they are being considered for a post in which they will have access to highly sensitive information or assets or as a part of clearance reinvestigations.

The United Kingdom has three levels of security vetting checks. The first type of check, the Counter Terrorist Check, is meant to be carried out if the individual is "working in proximity to public figures, or requires unescorted access to certain military, civil, industrial or commercial establishments assessed to be at particular risk from terrorist attack." The second type of check, known as a Security Check, aims to determine whether the individual's "character and personal circumstances are such that they can be trusted to work in a position which involves long-term, frequent and uncontrolled access to SECRET assets." The third type of check, Developed Vetting, is conducted as an add-on to the Security Check for individuals requiring "long term, frequent, and uncontrolled access to Top Secret information."² Vetting checks are aimed at understanding an individual's loyalty, honesty, and reliability, with specific focus on such vulnerabilities as bribery and blackmail.

Unique Features of the United Kingdom's Vetting Process

The United Kingdom uses the term *aftercare* to account for continuous monitoring and evaluation programs. The purpose of aftercare is to monitor potential security concerns between defined periods of clearance-holder reviews. Aftercare also includes the incorporation of "risk management measures" installed by agencies to monitor the "security reliability of individuals" holding a clearance.³

The UKSV defines its Baseline Personnel Security Standard as a preemployment control for all "civil servants, members of the Armed Forces, temporary staff and government contractors generally," or it is applied to "any individual who, in the course of their work, has access to government assets," appearing to mimic definitions of U.S. suitability standards.⁴

The United Kingdom also appears to be much more customer focused during the vetting process and has a series of customer-centric points contained within its vetting charter. For example, the UKSV allows subjects to review a written transcript of their vetting interview (both questions and answers to ensure accuracy), request a different vetting officer if they feel uncomfortable with the assigned officer (based on age, race, or gender differences), and request for friends and family to be present during questioning. The UKSV also continually gives customers (agencies), stakeholders (vetting

ity Vetting and the Foreign and Commonwealth Services National Security Vetting.

² UK Ministry of Defence, 2019.

³ UK Ministry of Defence, 2019.

⁴ UK Cabinet Office, *HMG Baseline Personnel Security Standard*, London, updated May 2018.

employees), and interviewees the chance to provide feedback about the overall vetting process to improve and advises individuals on what options are available for recourse—providing staff assistance to address grievances. The UKSV also uses forecast methods to fund and staff its ranks, since it “cannot accommodate large numbers of additional clearances on an ad hoc basis.”⁵

This section notes the main locations for finding publicly available information related to the UKSV’s vetting process and other important strategic documents that guide the overall UK security clearance process.

Centre for the Protection of National Infrastructure, website, undated.

<https://www.cpni.gov.uk/about-cpni>

This website serves as a repository of information relevant to protecting UK critical infrastructure. The Centre for the Protection of National Infrastructure is the official government authority tasked to provide protective security advice for all of the United Kingdom’s national infrastructure. The center appears to function in nearly the same way as DHS’s National Protection and Programs Directorate. The Centre for the Protection of National Infrastructure is directly accountable to the Security Service (MI5), the equivalent of the FBI’s domestic counterterrorism focus.

UK Cabinet Office, *Guidance on Departmental Information Risk Policy*, Version 1.1, London, April 2013.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/365968/Guidance_on_Departmental_Information_Risk_Policy_v1_1_Apr-13.pdf

This report reviews handling practices for sensitive data against the lens of the United Kingdom’s Data Handling Review report from 2008.⁶ That review presented a set of mandatory risk-policy standards for departments and agencies, guidance on how to monitor compliance and effectiveness of the risk policies identified, and additional risks associated with supply chain management.

UK Cabinet Office, *HMG Baseline Personnel Security Standard: Guidance on the Pre-Employment Screening of Civil Servants, Members of the Armed Forces, Temporary Staff and Government Contractors*, London, May 2018.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf

This report provides an in-depth description of the Baseline Personnel Security Standard preemployment screening practices for key cleared populations within the United Kingdom, and the report updated the Baseline Personnel Security Standard. It pro-

⁵ UK Ministry of Defence, 2019.

⁶ UK Cabinet Office, *Data Handling Procedures in Government*, London, June 2008.

vides preemployment control guidance derived from the UK Parliament's security policy framework,⁷ which calls for promoting a holistic view of security through supplementing Baseline Personnel Security Standard measures through the incorporation of physical and information technology measures. Lastly, this document highlights some of the key differences between the Baseline Personnel Security Standard and the National Security Vetting standards.

UK Cabinet Office, *HMG Personnel Security Controls, Version 4*, London, May 2018.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714017/HMG_Personnel_Security_Controls_-_May_2018.pdf

The *HMG Personnel Security Controls* guide describes the United Kingdom's personnel security and national security vetting policies and how the processes work, including (1) why and in what circumstances personnel security and national security vetting controls may be applied, (2) the type of information that individuals must provide, and (3) security clearance adjudication criteria. This guide also broadens the definition of *national security*; formerly, the United Kingdom considered national security to mean the "protection of the state and its vital interests from attacks by other states" but now should include "threats to the citizen and our way of life, as well as to the integrity and interests of the state more generally." This source also includes a detailed appendix on the types of security control, whom it applies to, and what types of screening are involved (similar to OPM's Position Designation Tool⁸).

UK Cabinet Office, *Government Security: Roles and Responsibilities*, London, November 2018.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/758358/20180919_GovernmentSecurityRolesAndResponsibilities.pdf

This document provides policy guidance implementing the results of the 2016 Transforming Government Security Review *intended* to transform ("simplify") UKSV security governance and accountability and the resulting overarching *Government Transformation Strategy*. The security transformation was largely intended to cease the operations of "legacy [security clearance] structures" and modernize various roles and responsibilities throughout government departments and stakeholder entities.⁹

⁷ UK Cabinet Office, "Security Policy Framework, May 2018," webpage, last updated May 24, 2018.

⁸ OPM, "Suitability Executive Agent: Position Designation Tool," webpage, undated.

⁹ The final review resulted in the official UK Cabinet Office, *Government Transformation Strategy*, London, February 9, 2017.

UK Ministry of Defence, “Guidance: United Kingdom Security Vetting,” webpage, last updated August 2, 2019.

<https://www.gov.uk/guidance/security-vetting-and-clearance>

This webpage provides an overview of the UK security clearance process and its three main security clearance levels for civil servants, military personnel, and contractors, as well as how employees may be sponsored for clearances by their employers and explanations of what to expect throughout the clearance process. This site also describes the preconditions and processes related to transfers (reciprocity) for cleared personnel within the country.

Australia

Overview

Much of the information regarding Australian vetting practices and procedures resides in a restricted form not generally available for public consumption. Therefore, this section lays out existing publicly available information regarding Australia’s security vetting organizations and practices, noting exemplary sources of information for U.S. Security, Suitability, and Credentialing manager consideration.

The Australian Government Security Vetting Agency (AGSVA) conducts vetting for all individuals requiring a security clearance. Individual government entities managed their own security vetting for employees (including contractors) until September 2010, when the Department of Defence decided to centralize its vetting practices in much the same way as the United Kingdom. The overarching consideration for consolidation was born out of desire to decrease costs associated with the vetting process and increase clearance reciprocity between agencies.

Australia’s Protective Security Policy Framework identifies security clearance standards at four different levels:¹⁰ (1) the Baseline level, which allows classified information access up to and including the Protected level;¹¹ (2) Negative Vetting 1 level, which permits access to classified information and resources up to and including Secret; (3) the Negative Vetting 2 level, which permits access to classified information and resources up to and including Top Secret; and (4) the Positive Vetting level, which allows access to resources at all classification levels, including “certain types of caveated and codeword information.”¹² The following resources provide more granularity on AGVSA’s policies regarding vetting and associated clearance levels, costs associated

¹⁰ Australian Attorney-General’s Department, “The Protective Security Policy Framework,” undated.

¹¹ Protected information may be akin to the U.S. For Official Use Only or Confidential level.

¹² Information regarding the types of checks and vetting conducted at these levels is not generally available to the public. See Australian Department of Defence, “Australian Government Security Vetting FAQ,” webpage, undated.

with background investigations, and other measures of performance reported by the vetting agency.

Unique Features of Australia's Vetting Process

Australia has a few features that set it apart from the way other FVEY partners conduct vetting. First, AGVSA manages a large (based on population size), 300-person contractor workforce that functions in various support roles. AGVSA uses regional vetting support centers across each of Australia's states and territories, where many of the contractors conduct operations. Second, given the relatively small size of government-associated vetting personnel, AGVSA has been forced to rely on the use of industry vetting panels that act as a surge capability within Australia's private sector to carry out vetting processes. The panels consist of 21 companies (approximately 200 personnel) that, as of 2015, were conducting more than 50 percent of Australia's of security clearance investigations.¹³ Third, AGVSA's noted capacity issues have caused a variety of security lapses, including a large number of applications that received waivers to reduce the investigation backlog and other cases in which a lack of AGVSA contractor oversight contributed to improper storage of personally identifiable information.¹⁴

¹³ Australian National Audit Office, *Central Administration of Security Vetting*, Canberra, June 2015.

¹⁴ AGVSA's capacity issues have been publicly reported both through news articles and official government reports. For example, in May 2018, the *Sydney Morning Herald* reported that, despite 43 percent of vetting assessments in 2015–2016 and 2016–2017 resulting in potential security concerns, “almost all decisions were made to allow the clearance without extra measures to reduce risks” (Sally Whyte, “Vetting Agency Not Protecting Against Internal Threats: Audit Report,” *Sydney Morning Herald*, May 12, 2018). The *Sydney Morning Herald* further noted that AGVSA did “not share information about the security concerns raised by the vetting process with the government department or agency where the staff member proposed to work, due to privacy concerns.” In October 2018, the *Canberra Times* began tracking developments related to a large number (“hundreds”) of security clearance waivers granted by an “entity” but did not directly attribute the waivers to AGVSA (Sally Whyte, “Hundreds of Waivers for Security Clearances Handed Out,” *Canberra Times*, October 9, 2018). The developing story was a result of statistics provided in a report by the Australian Attorney-General's Department, which cited that many of the waivers were handed out because of either noncitizenship or individuals with an “uncheckable background” (Australian Attorney-General's Department, *Protective Security Policy Framework: 2016–2017 Compliance Report*, Canberra, 2017). Further, the *Canberra Times* article noted that between 2015–2016 and 2016–2017, “the number of non-Australian citizens to be given security clearances doubled from 156 to 317.” A third article, from the *Sydney Morning Herald* in September 2018, noted the increased risk to personal information posed by the increased use of AGVSA contractors, who at the time of reporting consisted of 22 personnel conducting 85 percent of the security clearance applications (Fergus Hunter, “Alarm as Top-Level Security Vetting Is Being Outsourced to Private Contractors,” *Sydney Morning Herald*, September 3, 2018). The article notes that AGVSA's increased use of contractors was born out of an ever-increasing backlog of cases, which for Australia's highest personal vetting level was an approximate 15-month wait. Audits of the contracting agencies performing this work found that they were “frequently failing to properly secure the information.”

Australian Government Security Vetting Agency, “Corporate/Defence Industry Information and Policy,” webpage, undated.

<http://www.defence.gov.au/AGSVA/corporate-industry-policy.asp>

This webpage serves as an additional repository of information for AGSVA processes, including associated fees and charges to sponsoring agencies, service-level charters, explanations of how performance metrics are recorded, and foundational information contained within Australia’s primary national security documents.

Australian Government Security Vetting Agency, “Fact Sheets and Forms,” webpage, undated.

<http://www.defence.gov.au/AGSVA/factsheets-forms.asp>

This webpage serves as a repository of information for the four different levels of clearance. It describes what types of documents are required for each stage of the process, as well of some of the “aftercare” (continuous monitoring and continuous evaluation) associated with cleared employees.

Australian National Audit Office, *Central Administration of Security Vetting*, Canberra, June 2015.

<https://www.anao.gov.au/work/performance-audit/central-administration-security-vetting>

The objective of this 2015 audit report was to examine the efficiency and effectiveness of AGSVA vetting, and the report discusses various legislative reforms to Australia’s national security apparatus. The audit finds that AGSVA “commenced operations on the back foot, with significantly reduced vetting resources compared to those previously deployed across government, and without an appropriate management structure, documented procedures and adequate ICT [information and communications technology] systems . . . the failure to identify and address key risks during the policy development and implementation planning phases has had lasting consequences for AGSVA’s delivery of vetting services.”

Australian National Audit Office, *Mitigating Insider Threats Through Personnel Security: Across Entities*, Canberra, ANAO Report No. 38 2017-18, 2018.

https://www.anao.gov.au/sites/g/files/net5496/f/ANAO_Report_2017-2018_38.pdf

Although many of the audit reports mentioned throughout Australia’s newspaper coverage are likely not publicly available, this report offers insight into Australia’s Protective Security Policy Framework.¹⁵ The report outlines the set of security requirements mandated by Parliament and discusses eligibility and suitability requirements of potential government employees requiring a security clearance. It also examines some of the implications of the initial consolidation of vetting processes under AGVSA—

¹⁵ Australian Attorney-General’s Department, undated.

specifically, that the cost benefit of such a move had not yet materialized and did not adequately institute precautionary insider threat measures throughout the government.

Thom, Vivienne, *Inquiry into Allegations of Inappropriate Vetting Practices in the Defence Security Authority and Related Matters*, Canberra, Australia: Inspector General of Intelligence and Security, December 2011.

https://www.igis.gov.au/sites/default/files/files/Inquiries/docs/DSA_report.pdf

This earlier audit report, from 2011, follows the story of three whistle-blowers employed by the Defence Security Authority (one of the preceding AGVSA entities), drawing attention to “inappropriate vetting practices” that included “incorrect data entry.” The contractors’ alleged reports, confirmed by the internal audit cited, found that “difficulties in uploading data led to the use by vetting staff of ‘workarounds’ to address both database incompatibilities and situations where an applicant had not provided all of the data required,” and these “corrupted data had then entered the Australian Security Intelligence Organisation (ASIO)” and used for subsequent security assessments.

New Zealand

Overview

New Zealand’s Security Intelligence Service conducts security vetting of potential government employees in unison with New Zealand’s domestic intelligence organizations. Security Intelligence Service vetting personnel are the equivalent of U.S. military warrant officers. Security clearance decisions (and associated vetting processes) function within the national Protective Security Requirements (PSR) framework.¹⁶ The PSR contains 20 mandatory security requirements not only for New Zealand personnel but also for its physical and information security policies.

New Zealand does not use contractors in any part of the background investigation process, unlike security processes conducted within the rest of the FVEY community. All of New Zealand’s security vetting protocols exist at the Secret level or higher to protect the operational security of investigators and methods employed during investigations. PERSEC 21, the restricted document that New Zealand references to update and modernize its vetting practices, is the manner by which the government is “securing its workforce.”¹⁷ New Zealand also began conducting vetting customer satisfaction surveys instituted through its Security Clearance Enhancement Teams in 2016, although the results of such surveys are held at a restricted level.

¹⁶ Protective Security Requirements, homepage, undated.

¹⁷ Informal discussion with New Zealand official, December 21, 2018.

Unique Features of New Zealand's Vetting Process

The reciprocity agreements instituted within New Zealand afford great flexibility to employees needing or seeking work among different agencies requiring the same level of security clearance. One official we spoke with explained that, within the country, final security clearance decisions acted much in the same way as holding a U.S. driver's license—once obtained, it is assumed that a citizen can drive in any state. Security clearance decisions, once granted, are unchallenged by agencies within the country. Discussions with one high-ranking New Zealand official revealed that the range of current (and future) FVEY operations requires a mutually inclusive security view when such facilities are shared globally within the maritime, land, or air domain.¹⁸ However, instances of shared facilities are complicated as coalition forces are added to staff. The official stated that New Zealand also retains agreed standards on data access that allow for cleared individuals to rotate freely within the national security enterprise without the need for additional vetting requests for system access.

Another unique feature of New Zealand's vetting landscape is the limited amount of recourse options for employees denied a clearance. Since the New Zealand government does not officially abide by a written constitution, the country has a different security vetting litigation culture when compared with other FVEY countries; it instead relies on common law to administer or reexamine adjudication decisions. The Security Intelligence Service uses some additional terminology to define behavioral characteristics within the PSR framework, such as *strange* or *unusual behavior*.

New Zealand Security Intelligence Service, *Inquiry into Security Clearance Vetting Processes*, Wellington, 2010.

Although the initial section of this document focuses on the case of falsified testimony of one individual (the director of New Zealand's Defence Technology Agency), the remainder of the report provides excellent context for vetting conducted by NZSIS, including relevant legislation, a more granular view of the vetting process, and how oversight of the organization is conducted.

New Zealand Security Intelligence Service, *NZSIS 2016 Annual Report*, Wellington, 2016.

<https://www.nzsis.govt.nz/assets/media/nzsis-ar16.pdf>

This report discusses the role of the New Zealand Security Intelligence Service (NZSIS), including functions, security intelligence, foreign intelligence, and protective security advice. This document also characterizes the NZSIS role in vetting individuals for security clearances. NZSIS vetting officers undertake a range of duties, including interviewing candidates and referees, to make an assessment about an individual's suitability to hold a security clearance. In December 2014, the New Zealand cabinet

¹⁸ Informal discussion with New Zealand official, December 21, 2018.

approved the PSR, which includes mandatory vetting requirements for security governance, personnel security, information security, and physical security. The document explains that the PSR framework provides a single source of tools and guidance for agencies as they implement the PSR requirements. This report also discusses actions taken by the Security Clearance Enhancement, which was established to serve as a single point of contact about vetting for security clearance holders, candidates, and agencies. Separately, the report notes that a “vetting customer survey” was conducted in January 2016 to better understand how to improve the processes and functions of NZSIS vetting personnel.

New Zealand Security Intelligence Service, *Annual Report 2017*, Wellington, 2017.
<https://www.nzsis.govt.nz/assets/media/nzsis-ar17.pdf>

This report follows the 2016 annual report. The 2017 reports notes the creation of the Security Clearance Enhancement team, which reportedly helped foster engagement activities with vetting agencies and vetting candidates. A follow-up in June 2017 to the vetting survey conducted in January 2016 revealed a positive increase in the customer perceptions of NZSIS vetting practices. This report also notes that the recent uptick in vetting satisfaction has been enabled through (1) moving to a portfolio management approach for vetting customers (allowing a more customer-centric approach), (2) the hosting of an interagency vetting forum (the first for a number of years), and (3) the production of a monthly vetting newsletter. NZSIS is also working toward creating an introductory guide to the vetting process for new candidates to help candidates better understand the process.

Protective Security Requirements, “Overview of the Protective Security Requirements,” webpage, 2018.
<https://www.protectivesecurity.govt.nz/about-the-psr/overview-of-psr/>

This webpage provides policies regarding the management and protection of personnel, information, and physical assets within New Zealand’s public and private sectors. The PSR mandates compliance with a set of 20 requirements for all government agencies—but they are considered “best practice” items for other relevant sectors. For example, although “building security awareness” and “ensuring ongoing suitability” is a mandatory requirement for government agencies, understanding what “you need to protect” and “validating security measures” might be considered a best practice for public organizations.

Canada

Overview

The Canadian Security Intelligence Service (CSIS) functions as the primary investigation arm of the Canadian government, providing “security assessments on persons whose employment with the Government of Canada requires them to have lawful access to classified information or sensitive sites, such as major ports, airports, nuclear facilities or the Parliamentary Precinct.”¹⁹ Canada has four discrete levels of security classification: (1) Site Access (or Level 1), (2) Secret (or Level 2), (3) Top Secret (Level 3), and (4) and Enhanced Top Secret (Level 4). In addition to its vetting mission, CSIS (1) supports the Royal Canadian Mounted Police with the “accreditation process for Canadians and foreign nationals seeking access or participating in major events in Canada such as Olympic events, international summits and foreign visits”; (2) provides “security assessments to the Canada Border Services Agency (CBSA) with regard to drivers who apply for membership under the Canada-U.S. Free and Secure Trade (FAST) program”; and (3) provides “assessments to foreign governments, agencies and international organizations, such as NATO, with regard to Canadians seeking to work in sensitive positions abroad.”²⁰ The literature in this section describes CSIS’s associated support in these areas, in addition to its primary vetting missions. Canada also appears to use a form of specialized site-access clearances, as evidenced in the Canadian Nuclear Safety Commission report.

Unique Features of Canada’s Vetting Process

CSIS differentiates between suitability and security practices with the term *reliability status*. Reliability status provides a baseline level of suitability required to access restricted worksites. Both processes are evaluated according to individual reliability and loyalty to the Canadian government. In addition, all contractors must achieve reliability status prior to beginning work on government sites as part of the federal contracting process.

Canadian Nuclear Safety Commission, *Site Access Security Clearance for High-Security Sites*, draft report, Ottawa, GD-384, November 2012.

http://nuclearsafety.gc.ca/eng/pdfs/Draft-RD-GD/DRAFT-RDGD-384-Site-Access-Security-Clearance-for-High-Security-Sites_e.pdf

This draft report from the Canadian Nuclear Safety Commission outlines the specific personnel security measures required for unescorted privileges within protected sites, especially sites with nuclear material. The report uses the term *site access security clearance* (SASC) to define this type of access, but the term is not defined within the

¹⁹ Government of Canada, “Government Security Screening,” webpage, last updated July 18, 2018.

²⁰ Government of Canada, 2018.

literature provided by CSIS. The report states that the purpose of SASC is to “prevent unreasonable risk to high-security sites,” including “risks to operations, personnel, safety and national security from the insider threat.” Although the report does not discuss specifics, it suggests that the SASC program should set clear “threshold criteria” to trigger certain processes, which would be a parallel security screening process, separate from the regular government security screening process.

Government of Canada, “Apply for Security Screening for Your Personnel,” webpage, last updated May 28, 2019.

<https://www.tpsgc-pwgsc.gc.ca/esc-src/personnel/enquete-screening-eng.html>

This webpage highlights the procedural processes of both government and contracted employees required to access classified or other restricted space within Canada’s borders. This page also describes the various security screening standards CSIS uses to evaluate potential candidates. Lastly, this page describes, in some detail, the different types of protected information.

Royal Canadian Mounted Police, *Audit of Personnel Security*, Ottawa, July 2016.

<http://www.rcmp-grc.gc.ca/en/audit-personnel-security>

This audit report examines how one of the largest global police forces (30,000 employees, 25,000 contractors, and 17,000 volunteers) safeguards the integrity of its organization through a process known as the Departmental Security Program. Because the Royal Canadian Mounted Police is a robust organization, the initial vetting process for potential employees is rigorous, although “periodic security screening” does occur once accepted. This report discusses some of the struggles the Royal Canadian Mounted Police has faced as it has sought to modernize its security process (specifically, in reaction to budgetary and increased recruiting practices) and the associated steps the organization has taken toward increasing its overall vetting efficiency.

Security Intelligence Review Committee, *Broader Horizons: Preparing the Groundwork for Change in Security Intelligence Review*, Ottawa, Canada, 2015.

<http://www.sirc-csars.gc.ca/anrran/2014-2015/index-eng.html>

The Security Intelligence Review Committee (SIRC) is charged with acting as the external oversight body with reporting obligations regarding CSIS operations. This report focuses on a struggle between CSIS and SIRC regarding the number of insider threat deficiencies within CSIS purview. CSIS disagreed with the recommendations of the committee, forcing a “rarely-used clause in the CSIS Act” to “direct CSIS to conduct a review to gather information required for SIRC” to take additional steps.

Table of Bibliography Sources, by Category

This appendix lists all the literature presented throughout the main body of this annotated bibliography, organized by the category or section under which the document is binned. For each entry, Table A.1 indicates the primary category (chapter) under which the literature is organized; the section, if applicable, where the article is binned within a chapter; the title and format of the literature (e.g., book, PDF, website); year of the publication; type of source (e.g., government, academia); related categories or sections; whether the literature requires an access fee; and the URL.

Table A.1
Bibliography Sources, by Category

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Personnel Vetting Practices	Artificial Intelligence, Computational Tools, and Statistical Methods	<i>Machine Learning: The New AI</i> (book)	2016	Academia	Insider Threats	Yes	http://www.harvard.com/book/machine_learning_the_new_ai_the_mit_press_essential_knowledge_series/
					Continuous Monitoring and Continuous Evaluation		
Personnel Vetting Practices	Artificial Intelligence, Computational Tools, and Statistical Methods	"Using Genetic Algorithm to Minimize False Alarms in Insider Threats Detection of Information Misuse in Windows Environment," (webpage)	2014	Academia	Insider Threats	No	https://www.hindawi.com/journals/mpe/2014/179109/abs/
		<i>Artificial Intelligence and National Security</i> (PDF)			Insider Threats		
Personnel Vetting Practices	Artificial Intelligence, Computational Tools, and Statistical Methods	"User Identification and Authentication Using Multi-Modal Behavioral Biometrics" (PDF)	2014	Academia	Insider Threats	Yes	https://www.sciencedirect.com/science/article/pii/S0167404814000340
					Continuous Monitoring and Continuous Evaluation		
Personnel Vetting Practices	Artificial Intelligence, Computational Tools, and Statistical Methods	<i>Artificial Intelligence and National Security</i> (PDF)	2019	Government	Insider Threats	No	https://fas.org/sgp/crs/natsec/R45178.pdf
					Continuous Monitoring and Continuous Evaluation		

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Personnel Vetting Practices	Artificial Intelligence, Computational Tools, and Statistical Methods	"Modeling Human Behavior to Anticipate Insider Attacks" (PDF)	2011	Academia	Insider Threats	No	https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1249&context=jss
	Artificial Intelligence, Computational Tools, and Statistical Methods	"Android Forensics: Automated Data Collection and Reporting from a Mobile Device" (PDF)	2013	Academia	Not applicable	No	https://www.sciencedirect.com/science/article/pii/S1742287613000480
Personnel Vetting Practices	Artificial Intelligence, Computational Tools, and Statistical Methods	"Stress Level Detection via OSN Usage Pattern and Chronicity Analysis: An OSINT Threat Intelligence Module" (PDF)	2017	Academia	Cybervetting	No	https://www.infosec.aueb.gr/Publications/COSE%20Stress%20Detection%20-%20Site.pdf
	Artificial Intelligence, Computational Tools, and Statistical Methods	"Using Regression to Predict Potential Insider Threats" (PDF)	2018	Government	Insider Threats	Yes	https://www.dau.mil/library/arj/p/ARJ-85
Personnel Vetting Practices	Artificial Intelligence, Computational Tools, and Statistical Methods	"Surveillance of Anomaly and Misuse in Critical Networks to Counter Insider Threats Using Computational Intelligence" (PDF)	2015	Academia	Insider Threats	Yes	https://link.springer.com/article/10.1007/s10586-014-0403-y

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Personnel Vetting Practices	Artificial Intelligence, Computational Tools, and Statistical Methods	"Insider-Threat Detection Using Gaussian Mixture Models and Sensitivity Profiles" (PDF)	2018	Academia	Insider Threats	Yes	https://www.sciencedirect.com/science/article/pii/S0167404818302487
		"Autonomous Scientifically Controlled Screening Systems for Detecting Information Purposely Concealed by Individuals" (PDF)	2014	Academia	Continuous Monitoring and Continuous Evaluation Asset Protection	Yes	https://www.tandfonline.com/doi/full/10.1080/07421222.2014.995535
Personnel Vetting Practices	Artificial Intelligence, Computational Tools, and Statistical Methods	"Southern Illinois University Helps Create the World's First Centralized System for Evaluating Degrees, Licenses and Other Professional Credentials" (HTML, plain text)	2017	News article	Preinvestigation and Investigation	No	https://news.siu.edu/2017/12/121117-centralized-professional-credential-system.php
Personnel Vetting Practices	Behavioral Detection	"Improving Scrutiny of Applicants for Top Secret/SCI Clearances by Adding Psychological Assessments" (PDF)	2013	Academia	Preinvestigation and Investigation	No	https://www.nslj.org/wp-content/uploads/2_NatlSecLJ_252-300_Brickfield.pdf
Personnel Vetting Practices	Behavioral Detection	"Back to the Real: Efficacy and Perception of a Modified Cognitive Interview in the Field" (PDF)	2013	Academia	Preinvestigation and Investigation	Yes	https://onlinelibrary.wiley.com/doi/full/10.1002/acp.2942

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Personnel Vetting Practices	Behavioral Detection	<i>A Strategic Plan to Leverage the Social and Behavioral Sciences to Counter the Insider Threat</i> (PDF)	2018	Government	Preinvestigation and Investigation	No	https://apps.dtic.mil/dtic/tr/fulltext/u2/1063771.pdf
Personnel Vetting Practices	Behavioral Detection	<i>Improving Mental Health Reporting Practices in Between Personnel Security Investigations</i> (PDF)	2017	Government	Continuous Monitoring and Continuous Evaluation	No	https://www.dhra.mil/PERSEREC/Selected-Reports/#TR17-07
Personnel Vetting Practices	Behavioral Detection	<i>A Relevant Risk Approach to Mental Health Inquiries in Question 21 of the Questionnaire for National Security Positions (SF-86)</i> (PDF)	2015	Government	Preinvestigation and Investigation	No	https://www.dhra.mil/PERSEREC/Selected-Reports/#TR15-01
Personnel Vetting Practices	Behavioral Detection	<i>Minimizing Insider Threat Risk with Behavioral Monitoring</i> (PDF)	2018	Private sector	Insider Threats	Yes	https://www.ignited.global/case/business/minimizing-insider-threat-risk-behavioral-monitoring
Personnel Vetting Practices	Behavioral Detection	"Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis" (PDF)	2013	Academia	Insider Threats	Yes	https://www.jstor.org/stable/10.2979/eservicej.9.1.1067seq=1#page_scan_tab_contents

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Personnel Vetting Practices	Behavioral Detection	"A Human Factors Contribution to Countering Insider Threats: Practical Prospects from a Novel Approach to Warning and Avoiding" (PDF)	2017	Academia	Insider Threats	Yes	https://link.springer.com/article/10.1057/sj.2015.36
Personnel Vetting Practices	Behavioral Detection	"Trustworthiness Attribution: Inquiry into Insider Threat Detection" (PDF)	2018	Academia	Insider Threats Organizational Resiliency and Risk Assessment	Yes	https://asistdl.pericles-prod.literatmonline.com/doi/pdf/10.1002/asi.23938
Personnel Vetting Practices	Behavioral Detection	"Can Security Vetting Be Extended to Include the Detection of Financial Misconduct?" (PDF)	2017	Academia	Insider Threats Continuous Monitoring and Continuous Evaluation	Yes	https://www.tandfonline.com/doi/pdf/10.1080/10246029.2017.1294096
Personnel Vetting Practices	Behavioral Detection	"Efficacy of Modified Cognitive Interviewing, Compared to Human Judgments in Detecting Deception Related to Bio-Threat Activities" (PDF)	2013	Academia	Preinvestigation and Investigation Continuous Monitoring and Continuous Evaluation	No	https://scholarcommons.usf.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1249&context=jss
Personnel Vetting Practices	Behavioral Detection	"Strategy and Misdirection in Forced Choice Memory Performance Testing in Deception Detection" (PDF)	2017	Academia	Continuous Monitoring and Continuous Evaluation	Yes	https://onlinelibrary.wiley.com/doi/full/10.1002/acp.3310

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Personnel Vetting Practices	Behavioral Detection	"Applying Cognitive Models of Deception to National Security Investigations: Considerations of Psychological Research, Law, and Ethical Practice" (PDF)	2011	Academia	Preinvestigation and Investigation	No	https://heinonline.org/HOL/Page?handle=hein.journals/jpsych39&div=21&g_sent=1&casa_token=&collection=journals
		"Psychological Perspectives on Interrogation" (PDF)	2017	Academia	Preinvestigation and Investigation	No	https://journals.sagepub.com/doi/pdf/10.1177/1745691617706515
		"Cues to Deception and Ability to Detect Lies as a Function of Police Interview Styles" (PDF)	2007	Academia	Preinvestigation and Investigation	Yes	https://www.jstor.org/stable/4499551?seq=1#metadata_info_tab_contents
Personnel Vetting Practices	Social Media and Sentiment Analysis	"#EpicFail: How to Avoid Social Media Disasters in the Hiring Process" (PDF)	2015	Private sector	Cybervetting	No	http://www.mondaq.com/unitedstates/x/415174/employee+rights+labour+relations/EpicFail+How+To+Avoid+Social+Media+Disasters+In+The+Hiring+Process
Personnel Vetting Practices	Social Media and Sentiment Analysis	"How Often Is Employee Anger an Insider Risk? Detecting and Measuring Negative Sentiment Versus Insider Risk in Digital Communications" (PDF)	2013	Academia	Insider Threats	No	https://commons.erau.edu/jdfs/vol8/iss2/3/
					Organizational Resiliency and Risk Assessment		

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Personnel Vetting Practices	Social Media and Sentiment Analysis	"The Human Factor in the Social Media Security—Combining Education and Technology to Reduce Social Engineering Risks and Damages" (PDF)	2015	Academia	Asset Protection	No	https://www.sciencedirect.com/science/article/pii/S2351978915001821
Personnel Vetting Practices	Cybervetting	"Cybervetting, PersonEnvironment Fit, and Personnel Selection: Employers' Surveillance and Sensemaking of Job Applicants' online Information" (PDF)	2014	Academia	Not applicable	Yes	https://www.tandfonline.com/doi/full/10.1080/00909882.2014.954595
Personnel Vetting Practices	Cybervetting	<i>Cyber Culture and Personnel Security: Report II—Ethnographic Analysis of Second Life</i> (PDF)	2011	Government	Continuous Monitoring and Continuous Evaluation	No	https://apps.dtic.mil/dtic/tr/fulltext/u2/a568713.pdf
Personnel Vetting Practices	Cybervetting	<i>Cyberculture and Personnel Security: Report I—Orientation, Concerns, and Needs</i> (PDF)	2011	Government	Not applicable	No	https://www.dhra.mil/Portals/52/Documents/perserec/tr11-01.pdf
Personnel Vetting Practices	Cybervetting	<i>Developing a Cybervetting Strategy for Law Enforcement</i> (PDF)	2010	Government	Not applicable	No	http://www.iacpsocialmedia.org/wp-content/uploads/2017/02/CybervettingReport-2.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Personnel Vetting Practices	Cybervetting	"Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-Vetting and Law's Inability to Catch Up" (PDF)	2012	Academia	Not applicable	Yes	https://heinonline.org/HOL/Page?handle=hein.journals/johnmars12&div=23&g_sent=1&casa_token=&collection=journals
		"Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment" (PDF)	2018	Academia	Asset Protection	No	https://heinonline.org/HOL/Page?handle=hein.journals/johnmars12&div=23&g_sent=1&casa_token=&collection=journals
		"Cybervetting and Monitoring Employees' Online Activities: Assessing the Legal Risks for Employers" (PDF)	2010	Academia	Not applicable	No	https://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2010/annualconference/161.pdf
Personnel Vetting Practices	Cybervetting	"Predicting the Importance of Newsfeed Posts and Social Network Friends" (PDF)	2010	Academia	Preinvestigation and Investigation	No	http://maxchickering.com/publications/aaai10.pdf
		"Combining List Experiment and Direct Question Estimates of Sensitive Behavior Prevalence" (PDF)	2015	Academia	Not applicable	No	https://academic.oup.com/jssam/article/3/1/43/915561
Preinvestigation and Investigation	Vetting for Employment	"Risk Factors for Misconduct in a Navy Sample" (PDF)	2009	Academia	Not applicable	Yes	https://www.tandfonline.com/doi/full/10.1080/08995600902768776

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Preinvestigation and Investigation	Vetting for Employment	"The Predictive Value of Criminal Background Checks: Do Age and Criminal History Affect Time to Redemption?" (PDF)	2011	Academia	Not applicable	Yes	https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1745-9125.2010.00217.x
Preinvestigation and Investigation	Vetting for Employment	<i>The Truth Machine: A Social History of the Lie Detector</i> (book)	2012	Academia	Behavioral Detection	Yes	https://jhupbooks.press.jhu.edu/title/truth-machine
Preinvestigation and Investigation	Vetting for Employment	<i>Security Clearances and the Protection of National Security Information: Laws and Procedures</i> (HTML)	2000	Government	Behavioral Detection	No	https://apps.dtic.mil/dtic/tr/fulltext/u2/a388100.pdf
Preinvestigation and Investigation	Vetting for Employment	<i>Personnel Security Clearances: Preliminary Observations on Joint Reform Efforts to Improve the Governmentwide Clearance Eligibility Process</i> (PDF)	2008	Government	Not applicable	No	https://www.gao.gov/assets/130/120961.html
Preinvestigation and Investigation	Vetting for Employment	"Deception Detection Techniques Using Polygraph in Trials: Current Status and Social Scientific Evidence" (PDF)	2016	Academia	Behavioral Detection	Yes	https://www.ceeol.com/search/article-detail?id=466425
Preinvestigation and Investigation	Vetting for Employment	"Further Investigation Supports the Accuracy of Polygraph Examinations" (PDF)	2006	Academia	Behavioral Detection	No	https://search.proquest.com/docview/1947989317pq-origsite=gscholar

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Preinvestigation and Investigation	Vetting for Employment	"Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information" (PDF)	2011	Academia	Not applicable	No	https://www.cmu.edu/dietrich/sds/docs/loewenstein/StrangersPlane.pdf
Preinvestigation and Investigation	Vetting for Employment	"Expected Practices in Background Checking: Review of the Human Resource Management Literature" (PDF)	2009	Academia	Not applicable	Yes	https://link.springer.com/article/10.1007/s10672-009-9111-9
Preinvestigation and Investigation	Vetting for Employment	<i>Assessing the Use of Employment Screening for Sexual Assault Prevention</i> (PDF)	2017	Academia	Not applicable	No	https://www.rand.org/pubs/research_reports/RR1250.html
Preinvestigation and Investigation	Vetting for Employment	"The Detection Psychological Manifestations of Non-Verbal Communication by Interrogator" (PDF)	2014	Academia	Not applicable	No	https://www.sciencedirect.com/science/article/pii/S1877042813053883
Preinvestigation and Investigation	Vetting for Employment	"Accusatorial and Informal-Gathering Interview and Interrogation Methods: A Multi-Country Comparison" (PDF)	2018	Academia	Not applicable	Yes	https://www.tandfonline.com/doi/full/10.1080/1068316X.2018.1467909

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Preinvestigation and Investigation	Vetting for Employment	"Testing the Limits of Evidence Based Polygraph Practices" (PDF)	2016	Academia	Behavioral Detection	No	https://www.researchgate.net/profile/Raymond_Nelson/publication/299470504_Testing_the_Limits_of_Evidence_Based_Polygraph_Practices/links/570391a208aedbac12706e8d/links/570391a208aedbac12706e8d/Testing-the-Limits-of-Evidence-Based-Polygraph-Practices.pdf
Preinvestigation and Investigation	Vetting for Employment	<i>Security Clearance Vetting at the Portsmouth Site</i> (PDF)	2016	Government	Not applicable	No	https://www.oversight.gov/report/doe/security-clearance-vetting-portsmouth-site
Preinvestigation and Investigation	Vetting for Employment	<i>Management Alert—CBP Spends Millions Conducting Polygraph Examinations on Unsuitable Applicants</i> (PDF)	2017	Government	Not applicable	No	https://www.oig.dhs.gov/reports/2017/management-alert-cbp-spends-millions-conducting-polygraph-examinations-unsuitable
Preinvestigation and Investigation	Vetting for Employment	"Credibility Assessment: Preliminary Process Theory, the Polygraph Process, and Construct Validity" (PDF)	2015	Academia	Behavioral Detection	No	https://www.sciencedirect.com/science/article/pii/S0167876014001354
Preinvestigation and Investigation	Vetting for Employment	"The Right to Silence at Risk: Neuroscience-Based Lie Detection in the United Kingdom, India, and the United States" (PDF)	2010	Academia	Behavioral Detection	No	https://heionline.org/HOL/Page?handle=hein.journals/gwilr42&div=36&g_sent=1&casa_token=&collection=journals&t=1559239631

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Preinvestigation and Investigation	Vetting for Employment	"Is It Time to Kill the Detection Wizard? Emotional Intelligence Does Not Facilitate Deception Detection" (PDF)	2019	Academia	Behavioral Detection	Yes	https://www.sciencedirect.com/science/article/pii/S0191886918304689
Preinvestigation and Investigation	Vetting for Employment	"ESR Top Ten Background Check Trends" (HTML)	2014	Private sector	Not applicable	Yes	https://www.esrcheck.com/Tools-Resources/ESR-Top-Ten-Background-Check-Trends/
Preinvestigation and Investigation	Vetting for Employment	"How to Detect Deception? Arresting the Beliefs of Police Officers, Prosecutors and Judges" (PDF)	2003	Academia	Adjudication and Adjudication Bias	Yes	https://www.tandfonline.com/doi/abs/10.1080/10683160308138
Preinvestigation and Investigation	Vetting for Employment	<i>Personnel Security Clearances: Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations</i> (PDF)	2018	Government	Not applicable	No	https://www.gao.gov/products/GAO-18-431T
Preinvestigation and Investigation	Vetting for Employment	<i>Additional Mechanisms May Aid Federal Tax-Debt Detection</i> (PDF)	2015	Government	Continuous Monitoring and Continuous Evaluation	No	https://www.gao.gov/assets/670/669073.pdf
Preinvestigation and Investigation	Vetting for Employment	<i>Aviation Security: TSA Has Taken Steps to Improve Vetting of Airport Workers</i> (PDF)	2015	Government	Not applicable	No	https://www.gao.gov/products/GAO-15-704T

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Preinvestigation and Investigation	Vetting for Employment	<i>Criminal History Records: Additional Actions Could Enhance the Completeness of Records Used for Employment-Related Background Checks</i> (PDF)	2015	Government	Not applicable	No	https://www.gao.gov/products/GAO-15-162
Preinvestigation and Investigation	Vetting for Employment	<i>Security Clearances: Tax Debts Owed by DoD Employees and Contractors</i> (PDF)	2014	Government	Continuous Monitoring and Continuous Evaluation	No	https://www.gao.gov/assets/670/665052.pdf
Preinvestigation and Investigation	Vetting for Employment	<i>Personnel Security Clearances: Additional Guidance and Oversight Needed at DHS and DoD to Ensure Consistent Application of Revocation Process</i> (PDF)	2014	Government	Not applicable	No	https://www.gao.gov/assets/670/665595.pdf
Preinvestigation and Investigation	Vetting for Employment	<i>Payday Lending: Federal Law Enforcement Uses a Multilayered Approach to Identify Employees in Financial Distress</i> (PDF)	2011	Government	Continuous Monitoring and Continuous Evaluation	No	https://archive.org/stream/federal-law-enforcement-uses-a-multilayered/242350-federal-law-enforcement-uses-a-multilayered_djvu.txt
Preinvestigation and Investigation	Vetting for Employment	<i>DoD Personnel Clearances: Delays and Inadequate Documentation Found for Industry Personnel</i> (PDF)	2007	Government	Not applicable	No	https://www.gao.gov/products/GAO-07-842T

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Preinvestigation and Investigation	Vetting for Employment	"Safeguarding Our Nation's Secrets: Examining the Security Clearance Process" (HTML)	2013	Government	Not applicable	No	https://www.govinfo.gov/content/pkg/CHRG-113shrg82570/html/CHRG-113shrg82570.htm
Preinvestigation and Investigation	Vetting for Employment	<i>Detecting Lies and Deceit: The Psychology of Lying and Implications for Professional Practice</i> (book)	2011	Academia	Not applicable	Yes	https://www.wiley.com/en-us/Detecting+Lies+and+Deceit%3A+Pitfalls+and+Opportunities%2C+2nd+Edition-p-9780470516249
Preinvestigation and Investigation	Vetting for Employment	"Asking Sensitive Questions: An Evaluation of the Randomized Response Technique Versus Direct Questioning Using Individual Validation Data" (PDF)	2013	Academia	Not applicable	No	https://www.wiley.com/en-us/Detecting+Lies+and+Deceit%3A+Pitfalls+and+Opportunities%2C+2nd+Edition-p-9780470516249
Preinvestigation and Investigation	Vetting for Employment	"Detecting Truth, Deception, and Innocence in a Mock Counter-Terrorism Scenario: The Use of Forced-Choice Testing" (PDF)	2018	Academia	Not applicable	Yes	https://www.tandfonline.com/doi/full/10.1080/18335330.2018.1438640
Preinvestigation and Investigation	Privacy, Civil Liberties, and Legal Concerns	"Cybervetting, Online Information, and Personnel Selection: New Transparency Expectations and the Emergence of a Digital Social Contract" (PDF)	2014	Academia	Cybervetting	Yes	https://journals.sagepub.com/doi/pdf/10.1177/0893318914541966

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Preinvestigation and Investigation	Privacy, Civil Liberties, and Legal Concerns	"The Insider Threat and Employee Privacy: An Overview of Recent Case Law" (PDF)	2013	Academia	Not applicable	No	https://rampages.us/keckjw/wp-content/uploads/sites/2169/2015/02/20130000The-insider-threat-and-employee-privacy-An-overview-of-recent-case-law.pdf
Preinvestigation and Investigation	Privacy, Civil Liberties, and Legal Concerns	DoD Security Clearance Adjudication and Appeal Process (PDF)	2003	Government	Adjudication and Adjudication Bias	No	https://fas.org/sgp/othergov/dod/dodig1203.pdf
Preinvestigation and Investigation	Privacy, Civil Liberties, and Legal Concerns	"The Standards of Conduct as Applied to Personal Social Media Use, Legal Advisory" (PDF)	2015	Government	Cybervetting	No	https://www.oge.gov/web/oge/nsf/016D5B5EB7E5DE11A85257E96005F5FBF13/\$FILE/LA-15-03-2.pdf
Preinvestigation and Investigation	Privacy, Civil Liberties, and Legal Concerns	Privacy: OPM Should Better Monitor Implementation of Privacy-Related Policies and Procedures for Background Investigations (PDF)	2010	Government	Not applicable	No	https://www.gao.gov/products/GAO-10-849
Preinvestigation and Investigation	Privacy, Civil Liberties, and Legal Concerns	"Employer Liability for Using Social Media in Hiring Decisions" (PDF)	2016	Academia	Cybervetting	No	https://www.researchgate.net/publication/305729785_Employer_Liability_for_Using_Social_Media_in_Hiring_Decisions
Preinvestigation and Investigation	Privacy, Civil Liberties, and Legal Concerns	"Is Cybervetting Ethical? An Overview of Legal and Ethical Issues" (PDF)	2017	Academia	Cybervetting	No	http://www.aabri.com/manuscripts/172677.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Adjudication and Adjudication Bias	Adjudication Guidelines and Practices	<i>Tier 1 and Tier 3 eAdjudication Business Rule Validation</i> (PDF)	2018	Government	Not applicable	No	https://www.dhra.mil/Portals/52/Documents/perserec/reports/TR-18-06_Tier_1_and_Tier_3_eAdjudication_Business_Rule_Validation.pdf
Adjudication and Adjudication Bias	Adjudication Guidelines and Practices	<i>Adjudicative Desk Reference Assisting Security Clearance Adjudicators, Investigators, and Security Managers in Implementing the U.S. Government Personnel Security Program</i>	2014	Government	Not applicable	No	https://www.dhra.mil/Portals/52/Documents/perserec/ADR_Version_4.pdf
Adjudication and Adjudication Bias	Adjudication Guidelines and Practices	<i>2016 RADAR Adjudication Quality Evaluation</i> (PDF)	2016	Government	Not applicable	No	https://www.dhra.mil/Portals/52/Documents/perserec/reports/MR-18-03_RADAR_2016_Adjudication_Quality_Evaluation_Report.pdf
Adjudication and Adjudication Bias	Adjudication Guidelines and Practices	<i>National Security Adjudicative Guidelines</i> (Security Executive Agent Directive 4) (PDF)	2017	Government	Not applicable	No	https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf
Adjudication and Adjudication Bias	Adjudication Bias	"Secrecy News: Security Clearance Denials and Constitutional Rights" (PDF)	2013	Academia	Not applicable	No	https://fas.org/blogs/secrecy/2013/09/hegab-cert/
Adjudication and Adjudication Bias	Adjudication Bias	"Individual Differences in Judging Deception: Accuracy and Bias" (PDF)	2008	Academia	Not applicable	No	http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.879.8829&rep=rep1&type=pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Adjudication and Adjudication Bias	Adjudication Bias	"Say What? How Unconscious Bias Affects Our Perceptions, Non-Profit Risk Management Sector" (HTML, plain text)	Undated	Private sector	Not applicable	No	https://nonprofitrisk.org/resources/news/say-what-how-unconscious-bias-affects-our-perceptions/
Adjudication and Adjudication Bias	Adjudication Bias	"Bias and Perception: How It Affects Our Judgment in Decision Making and Analysis" (HTML, plain text)	Undated	Academia	Not applicable	No	https://www.scribd.com/document/183174946/Small-Wars-Journal-Bias-and-Perception-How-It-Affects-Our-Judgment-in-Decision-Making-and-Analysis-2013-07-12
Adjudication and Adjudication Bias	Adjudication Legal Concerns	<i>Greene v. McElroy</i> (1959), Department of the Navy v. Egan (1988), <i>Webster v. Doe</i> (1988), <i>Perez v. Federal Bureau of Investigation</i> (1989), <i>Makky v. Chertoff</i> (2008), <i>El-Ganayni v. U.S. Department of Energy</i> (2010), and <i>Berry v. Conyers and Northover</i> (combined appeals in 2012) (HTML, plain text)	1959–2012	Government	Preinvestigation and Investigation Continuous Monitoring and Evaluation Credentialing	No	Available at https://law.justia.com
Suitability, Fitness, and Contractor Vetting	Suitability and Fitness Practices	<i>Doing Business with DHS: Industry Recommendations to Improve Contractor Employee Vetting</i> (PDF)	2018	Private sector	Contractor Vetting	No	https://www.insaonline.org/wp-content/uploads/2018/02/Charles-Allen_Prepared-Testimony-on-DHS-Vetting-27Feb2018.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Suitability, Fitness, and Contractor Vetting	Suitability and Fitness Practices	<i>Department of Defense Suitability and Fitness Guide, Procedures and Guidance for Civilian Employment Suitability and Fitness Determinations within the Department of Defense</i> (PDF)	2016	Government	Adjudication and Adjudication Bias	No	https://www.dhra.mil/Portals/52/Documents/perserec/DoD_Suitability_Guide_Version_1.0.pdf
	Suitability and Fitness Practices	<i>DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees</i> (PDF)	2012	Government	Adjudication and Adjudication Bias	No	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/140025/140025v731.pdf
Suitability, Fitness, and Contractor Vetting	Suitability and Fitness Practices	<i>Baseline Suitability Analysis</i> (PDF)	2013	Government	Adjudication and Adjudication Bias	No	https://www.dhra.mil/Portals/52/Documents/perserec/tr13-05.pdf
Suitability, Fitness, and Contractor Vetting	Suitability and Fitness Practices	<i>The Department of Homeland Security Personnel Suitability and Security Program</i> (PDF)	2012	Government	Adjudication and Adjudication Bias	No	https://www.dhs.gov/sites/default/files/publications/Instruction%20Handbook%20121-01-007%20Personnel%20Suitability%20and%20Security%20Program.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Suitability, Fitness, and Contractor Vetting	Suitability and Fitness Practices	<i>Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information</i> (Executive Order 13467) (PDF, HTML, plain text)	2008	Government	Adjudication and Adjudication Bias	No	https://fas.org/irp/offdocs/eo/eo-13467.htm
	Suitability and Fitness Practices	<i>Suitability and Security Process Review: Report to the President</i> (PDF)	2014	Government	Preinvestigation and Investigation Adjudication and Adjudication Bias Information Sharing and Reciprocity	No	https://www.archives.gov/files/isoo/oversight-groups/nisp/2014-suitability-and-processes-report.pdf
Suitability, Fitness, and Contractor Vetting	Suitability and Fitness Practices	<i>Security and Suitability Process Reform</i> (PDF)	2008	Government	Adjudication and Adjudication Bias Information Sharing and Reciprocity	No	https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/reports/joint_security_dec2008.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Suitability, Fitness, and Contractor Vetting	Suitability and Fitness Practices	"Position Designation System" (PDF, HTML)	Undated	Government	Preinvestigation and Investigation	No	https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/
					Adjudication and Adjudication Bias		
Suitability, Fitness, and Contractor Vetting	Contractor Vetting	<i>National Industrial Security Program Operating Manual</i> (PDF)	2016	Government	Asset Protection	No	https://fas.org/sgp/library/nispom/nispom2006.pdf
Suitability, Fitness, and Contractor Vetting	Contractor Vetting	<i>Operational Contract Support: Additional Actions Needed to Manage, Account for, and Vet Defense Contractors in Africa</i> (PDF)	2015	Government	Preinvestigation and Investigation	No	https://www.gao.gov/products/GAO-16-105
Suitability, Fitness, and Contractor Vetting	Contractor Vetting	<i>Operational Contract Support: Actions Needed to Address Contract Oversight and Vetting of Non-U.S. Vendors in Afghanistan</i> (PDF)	2011	Government	Preinvestigation and Investigation	No	https://www.gao.gov/products/GAO-11-771T
					Adjudication and Adjudication Bias		
					Asset Protection		

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Suitability, Fitness, and Contractor Vetting	Contractor Vetting	<i>Contract Security Guards: Army's Guard Program Requires Greater Oversight and Reassessment of Acquisition Approach</i> (PDF)	2006	Government	Adjudication and Adjudication Bias Asset Protection	No	https://www.gao.gov/products/GAO-06-284
	Insider Threats	<i>Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage</i> (PDF)	2005	Government	Asset Protection	No	https://fas.org/sgp/othergov/dod/insider.pdf
Insider Threat	Insider Threat Practices and Challenges	<i>A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector</i> (PDF)	2013	Private sector	Not applicable	No	https://www.insonline.org/a-preliminary-examination-of-insider-threat-programs-in-the-u-s-private-sector/
Insider Threat	Insider Threat Practices and Challenges	<i>Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Posture of the U.S. Departments and Agencies Be Improved</i> (PDF)	2019	Academia	Continuous Monitoring and Continuous Evaluation	No	https://www.rand.org/pubs/research_reports/RR2684.html
Insider Threats	Insider Threat Practices and Challenges	<i>"Insider Threat: Policy Impact and Overview"</i> (PDF)	2018	Private sector	Not applicable	No	https://www.insonline.org/a-preliminary-examination-of-insider-threat-programs-in-the-u-s-private-sector/

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Insider Threats	Insider Threat Practices and Challenges	<i>Summary of Federal Citations for the National Insider Threat Task Force</i> (PDF)	2019	Government	Preinvestigation and Investigation Adjudication and Adjudication Bias	No	https://www.dni.gov/files/NCSC/documents/nittf/Summary_of_Federal_Agencies_Security_Legal_Authorities.pdf
Insider Threats	Insider Threat Practices and Challenges	<i>Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards</i> (PDF)	2017	Government	Not applicable	No	https://www.dni.gov/files/NCSC/documents/nittf/NITTf-Insider-Threat-Guide-2017.pdf
Insider Threats	Insider Threat Practices and Challenges	<i>National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs</i> (PDF)	2012	Government	Asset Protection	No	https://fas.org/sgp/obama/insider.pdf
Insider Threats	Detection and Prevention Mechanisms	<i>Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis</i> (PDF)	2006	Academia	Asset Protection	No	https://resources.sei.cmu.edu/asset_files/TechnicalReport/2006_005_001_14798.pdf
Insider Threats	Detection and Prevention Mechanisms	<i>Secrecy in U.S. National Security: Why a Paradigm Shift Is Needed</i> (PDF)	2018	Academia	Not applicable	No	https://www.rand.org/pubs/perspectives/PE305.html

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Insider Threats	Detection and Prevention Mechanisms	<i>Fixing Leaks: Assessing the Department of Defense's Approach to Preventing and Deterring Unauthorized Disclosures</i> (PDF)	2013	Academia	Asset Protection	No	https://www.rand.org/pubs/research_reports/RR409.html
Insider Threats	Detection and Prevention Mechanisms	<i>DoD Insider Threat Mitigation</i> (PDF)	Undated	Government	Asset Protection	No	https://apps.dtic.mil/dtic/tr/fulltext/u2/a391380.pdf
Insider Threats	Detection and Prevention Mechanisms	<i>Violence in the Federal Workplace: A Guide for Prevention and Response</i> (PDF)	2013	Government	Organizational Resiliency and Risk Assessment	No	https://www.dhs.gov/sites/default/files/publications/ISC%20Violence%20in%20the%20Federal%20Workplace%20Guide%20April%202013.pdf
Insider Threats	Detection and Prevention Mechanisms	<i>Modeling Insider Threat from the Inside and Outside: Individual and Environmental Factors Examined Using Event History Analysis</i> (PDF)	2018	Government	Not applicable	No	https://www.dhra.mil/Portals/52/Documents/perserec/reports/TR-18-14_Modeling_Insider_Threat_From_the_Inside_and_Outside.pdf
Insider Threats	Detection and Prevention Mechanisms	<i>Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders; Analysis and Observations</i> (PDF)	2005	Government	Asset Protection	No	https://www.dhra.mil/Portals/52/Documents/perserec/tr05-13.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Insider Threats	Detection and Prevention Mechanisms	<i>An Assessment of Data Analytics Techniques for Insider Threat Programs: Practitioner Views on Intelligence Program Design and Implementation (PDF)</i>	2018	Private sector	Not applicable	No	https://www.insaonline.org/wp-content/uploads/2018/08/INSA_Insider-Threat_Data-Analytics-July-2018.pdf
Insider Threats	Detection and Prevention Mechanisms	<i>Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation (PDF)</i>	2017	Private sector	Continuous Monitoring and Continuous Evaluation	No	https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Mind_Insider_FIN.pdf
Insider Threats	Detection and Prevention Mechanisms	<i>The Use of Publicly Available Electronic Information for Insider Threat Monitoring (PDF)</i>	2019	Private sector	Social Media and Sentiment Analysis	No	https://www.insaonline.org/wp-content/uploads/2019/02/FINAL-PAEI-whitepaper.pdf
Insider Threats	Detection and Prevention Mechanisms	<i>Insider Threat Workshop Proceedings: Papers and Presentations from the CSIAC Insider Threat Workshop (PDF)</i>	2013	Academia	Not applicable	No	https://www.csiac.org/wp-content/uploads/2016/03/CSIAC-Insider-Threat-Report-Proceedings.pdf
Insider Threats	Detection and Prevention Mechanisms	<i>Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks (PDF)</i>	2016	Government	Asset Protection	No	https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Insider Threats	Detection and Prevention Mechanisms	<i>Workplace Violence: Issues in Response</i> (PDF)	2003	Government	Organizational Resiliency and Risk Assessment	No	https://www.fbi.gov/file-repository/stats-services-publications-workplace-violence-workplace-violence/view
Insider Threats	Detection and Prevention Mechanisms	"Bad Apples or Bad Barrels: An Examination of Group- and Organizational-Level Effects in the Study of Counterproductive Work Behavior" (PDF)	2011	Academia	Organizational Resiliency and Risk Assessment	Yes	https://journals.sagepub.com/doi/10.1177/1059601110390998
Insider Threats	Detection and Prevention Mechanisms	<i>Insider Threat Mitigation Guidance</i> (PDF)	2015	Academia	Not applicable	No	https://www.sans.org/reading-room/whitepapers/monitoring/insider-threat-mitigation-guidance-36307
Insider Threats	Detection and Prevention Mechanisms	"Application of the Critical-Path Method to Evaluate Insider Risks" (PDF)	2015	Government	Not applicable	No	https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-2/pdfs/Shaw-Critical%20Path-June-2015.pdf
Insider Threats	Detection and Prevention Mechanisms	<i>Common Sense Guide to Mitigating Insider Threats</i> (PDF)	2012	Academia	Asset Protection	No	https://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf
Insider Threats	Detection and Prevention Mechanisms	"The Dimensionality of Counterproductivity: Are All Counterproductive Behaviors Created Equal?" (PDF)	2006	Academia	Organizational Resiliency and Risk Assessment	Yes	https://www.sciencedirect.com/science/article/pii/S0001879105001284

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Insider Threats	Detection and Prevention Mechanisms	"Detecting Insider Threats Through Language Change" (PDF)	2013	Academia	Continuous Monitoring and Continuous Evaluation	Yes	https://psycnet.apa.org/record/2013-20282-001
Insider Threats	Cloud-Based Insider Threats	"A Multidimension Taxonomy of Insider Threats in Cloud Computing" (PDF)	2016	Academia	Asset Protection	Yes	https://academic.oup.com/comjnl/article/59/11/1612/2433249
Insider Threats	Cloud-Based Insider Threats	"Cloud-of-Things Meets Mobility-as-a-Service: An Insider Threat Perspective" (PDF)	2018	Academia	Asset Protection	No	https://www.sciencedirect.com/science/article/pii/S0167404817302134
Insider Threats	Cloud-Based Insider Threats	"An Insider Threat Aware Access Control for Cloud Relational Databases" (PDF)	2017	Academia	Asset Protection	Yes	https://www.sciencedirect.com/science/article/pii/S0167404817302134
Continuous Monitoring and Continuous Evaluation	Not applicable	<i>The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security</i> (PDF)	2013	Government	Not applicable	No	https://apps.dtic.mil/dtic/tr/fulltext/u2/a626819.pdf
Continuous Monitoring and Continuous Evaluation	Not applicable	<i>Insider Risk Evaluation and Audit</i> (PDF)	2009	Government	Not applicable	No	https://www.nsi.org/pdf/reports/Insider%20Risk%20Evaluation.pdf
Continuous Monitoring and Continuous Evaluation	Not applicable	<i>FedRAMP Continuous Monitoring Strategy Guide</i> (PDF)	2018	Government	Not applicable	No	https://www.nsi.org/pdf/reports/Insider%20Risk%20Evaluation.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Continuous Monitoring and Continuous Evaluation	Not applicable	<i>Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation</i> (PDF)	2017	Private sector	Insider Threats	No	https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Mind_Insider_FIN.pdf
Continuous Monitoring and Continuous Evaluation	Not applicable	<i>Continuous Evaluation</i> (Security Executive Agent Directive 6) (PDF)	2018	Government	Insider Threats	No	https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-6-continuous%20evaluation-U.pdf
Continuous Monitoring and Continuous Evaluation	Not applicable	<i>Personnel Security Clearances: Plans Needed to Fully Implement and Oversee Continuous Evaluation of Clearance Holders</i> (PDF)	2017	Government	Not applicable	No	https://www.gao.gov/products/GAO-18-117
Continuous Monitoring and Continuous Evaluation	Not applicable	<i>Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain</i> (PDF)	2011	Government	Asset Protection	No	https://www.gao.gov/products/GAO-11-149
Trust in the Workplace	Trust in the Workforce	"Trust as a Human Factor in Holistic Cyber Security Risk Assessment" (PDF)	2015	Academia	Organizational Resiliency and Risk Assessment	No	https://www.researchgate.net/profile/Diane_Henshel/publication/283960105_Trust_as_a_Human_Factor_in_Holistic_Cyber_Security_Risk_Assessment/links/58cc8f384585157b6dac12f3/Trust-as-a-Human-Factor-in-Holistic-Cyber-Security-Risk-Assessment.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Trust in the Workplace	Trust in the Workforce	"Building a 21st Century Trusted Workforce" (PDF)	2018	Private sector	Organizational Resiliency and Risk Assessment	No	https://www.insaonline.org/wp-content/uploads/2018/11/Building-A-21st-Century-Trusted-Workforce-Transcript.pdf
Trust in the Workplace	Trust in the Workforce	"An Integrative Model of Organizational Trust" (PDF)	1995	Academia	Organizational Resiliency and Risk Assessment	No	https://www.jstor.org/stable/pdf/258792.pdf
Trust in the Workplace	Trust in the Workforce	<i>Credibility Assessment: Scientific Research and Applications</i> (PDF)	2014	Academia	Organizational Resiliency and Risk Assessment	Yes	https://www.elsevier.com/books/credibility-assessment/raskin/978-0-12-394433-7
Trust in the Workplace	Trust in the Workforce	"Trash-Talking: Competitive Incivility Motivates Rivalry, Performance, and Unethical Behavior" (PDF)	2018	Academia	Organizational Resiliency and Risk Assessment	No	https://www.sciencedirect.com/science/article/pii/S0749597816301157
Trust in the Workplace	Modeling Trust	"Increasing the Veracity of Event Detection on Social Media Networks Through User Trust Modeling" (PDF)	2014	Academia	Cybervetting	No	https://www.researchgate.net/publication/268147653_Increasing_the_Veracity_of_Event_Detection_on_Social_Media_Networks_Through_User_Trust_Modeling
Trust in the Workplace	Modeling Trust	"A Survey on Trust Modeling" (PDF)	2015	Academia	Not applicable	No	https://www.researchgate.net/profile/Jin_Hee_Cho4/publication/283670108_A_Survey_on_Trust_Modeling/links/56686b8a08ae7dc2ad36bd7.pdf
Trust in the Workplace	Modeling Trust	"An Adaptive Probabilistic Trust Model and Its Evaluation" (PDF)	2008	Academia	Organizational Resiliency and Risk Assessment	Yes	https://dl.acm.org/citation.cfm?id=1402905

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Trust in the Workplace	Other Characteristics of Trust (Personalities and Building Trust)	"Identifying Personality Traits to Enhance Trust Between Organisations: An Experimental Approach" (PDF)	2008	Academia	Organizational Resiliency and Risk Assessment Continuous Monitoring and Continuous Evaluation	Yes	https://onlinelibrary.wiley.com/doi/abs/10.1002/mde.1415
Trust in the Workplace	Other Characteristics of Trust (Personalities and Building Trust)	"Personality Traits and the Propensity to Trust Friends and Strangers" (PDF)	2016	Academia	Not applicable	Yes	https://www.sciencedirect.com/science/article/pii/S0362331915001123
Trust in the Workplace	Other Characteristics of Trust (Personalities and Building Trust)	"How to Build Trust in an Organization" (PDF)	2012	Academia	Organizational Resiliency and Risk Assessment	No	https://www.slideshare.net/BusinessEssentials/how-to-build-trust-in-an-organization
Trust in the Workplace	Other Characteristics of Trust (Personalities and Building Trust)	"The New Technologies in Personality Assessment: A Review" (PDF)	2018	Academia	Not applicable	Yes	https://psycnet.apa.org/record/2018-17017-001
Trust in the Workplace	Other Characteristics of Trust (Personalities and Building Trust)	"Who Is Trustworthy? Predicting Trustworthy Intentions and Behavior" (PDF)	2018	Academia	Organizational Resiliency and Risk Assessment	Yes	https://psycnet.apa.org/record/2018-33235-001?doi=1

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Trust in the Workplace	Other Characteristics of Trust (Personalities and Building Trust)	"Getting to Know You: A Longitudinal Examination of Trust Cues and Trust Development During Socialization" (PDF)	2017	Academia	Organizational Resiliency and Risk Assessment	Yes	https://journals.sagepub.com/doi/full/10.1177/0149206314543475
Trust in the Workplace	Other Characteristics of Trust (Personalities and Building Trust)	"The Traits One Can Trust: Dissecting Reciprocity and Kindness as Determinants of Trustworthy Behavior" (PDF)	2015	Academia	Organizational Resiliency and Risk Assessment	Yes	https://www.ncbi.nlm.nih.gov/pubmed/26330455
Trust in the Workplace	Other Characteristics of Trust (Personalities and Building Trust)	"The Psychology of Espionage" (PDF)	2017	Government	Insider Threats	No	https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-61-no-2/pdfs/psychology-of-espionage.pdf
Asset Protection	Places	<i>NIPP 2013: Partnering for Critical Infrastructure Security and Resilience</i> (PDF)	2013	Government	Not applicable	No	https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf
Asset Protection	Places	<i>National Strategy for the Physical Protection of Critical Infrastructures and Key Assets</i> (PDF)	2003	Government	Not applicable	No	https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf
Asset Protection	Places	<i>Risk Assessment Methodologies for Critical Infrastructure Protection, Part I: A State of the Art</i> (PDF)	2012	Government (Foreign)	Not applicable	No	https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Asset Protection	Places	<i>Protection of "Critical Infrastructure" and the Role of Investment Policies Relating to National Security</i> (PDF)	2008	Government (Foreign)	Not applicable	No	https://www.oecd.org/daf/inv/investment-policy/40700392.pdf
Asset Protection	Places	<i>Physical Security and Why It Is Important</i> (PDF)	2016	Academia	Not applicable	No	https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120
Asset Protection	Physical Assets	"Man-at-the-End Attacks: Analysis, Taxonomy, Human Aspects, Motivation and Future Directions" (PDF)	2015	Academia	Insider Threats	No	https://www.researchgate.net/publication/278730778_Man-At-The-End_Attacks
Asset Protection	Physical Assets	"An Adaptive Risk Management and Access Control Framework to Mitigate Insider Threats" (PDF)	2013	Academia	Insider Threats	Yes	https://dl.acm.org/citation.cfm?id=2622880
Asset Protection	Physical Assets	"Assessing Risk" (PDF)	2018	Academia	Not applicable	No	http://www.businessofgovernment.org/sites/default/files/Chapter%20Seven%20Assessing%20Risk.pdf
Asset Protection	Physical Assets	"U.S. European Command Needs to Improve Oversight of the Golden Sentry Program" (PDF)	2017	Government	Personnel Vetting Practices	No	https://www.dodig.mil/reports.html/Article/1119358/us-european-command-needs-to-improve-oversight-of-the-golden-sentry-program-red/

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Asset Protection	Physical Assets	"High Risk Non-Initiating Insider Identification Based on EEG Analysis for Enhancing Nuclear Security" (PDF)	2018	Academia	Insider Threats	Yes	https://www.sciencedirect.com/science/article/pii/S0306454917304218
Asset Protection	Information and Intellectual Property	"Reform of the Intelligence Community Prepublication Review Process: Balancing First Amendment Rights and National Security Interests" (PDF)	2016	Academia	Not applicable	No	https://www.nslj.org/wp-content/uploads/Bailey-Article-from-Vol.-5-Issue-2-complete-issue.pdf
Asset Protection	Information and Intellectual Property	<i>Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information</i> (Executive Order 13587) (HTML, plain text)	2011	Government	Not applicable	No	https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net
Asset Protection	Information and Intellectual Property	<i>Too Much Information: Misconfigured FTP, SMB, Rsync, and S3 Buckets Exposing 1.5 Billion Files</i> (PDF)	2018	Private sector	Not applicable	No	https://info.digitalshadows.com/rs/457-XEY-671/images/DigitalShadows-Research-DataExposure.pdf
Asset Protection	Information and Intellectual Property	"Data Breach at a University: Preparing Our Networks" (PDF)	2016	Academia	Cyber Security Insider Threats	No	https://www.nslj.org/wp-content/uploads/Spring-Symposium_Final_Website_2017-06-18.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Asset Protection	Information and Intellectual Property	"Hacking Federal Cybersecurity Legislation: Reforming the Effective Security of Federal Information Systems" (PDF)	2015	Academia	Cyber Security	No	https://www.nslj.org/wp-content/uploads/4_NatlSecLJ_345-385_Smith.pdf
Asset Protection	Information and Intellectual Property	<i>Protecting Classified Information: Defense Security Service Should Address Challenges as New Approach Is Piloted</i> (PDF)	2018	Government	Not applicable	No	https://www.gao.gov/products/GAO-18-407
Asset Protection	Information and Intellectual Property	<i>Information Security: OPM Has Improved Controls, but Further Efforts Are Needed</i> (PDF)	2017	Government	Not applicable	No	https://www.gao.gov/products/GAO-17-614
Asset Protection	Information and Intellectual Property	<i>Defense Acquisitions, Knowledge of Software Suppliers Needed to Manage Risks</i> (PDF)	2004	Government	Not applicable	No	https://www.gao.gov/products/GAO-04-678
Asset Protection	Information and Intellectual Property	"Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives" (PDF)	2018	Academia	Insider Threats Organizational Resiliency and Risk Assessment	Yes	https://onlinelibrary.wiley.com/doi/full/10.1111/isj.12129

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Organizational Resiliency and Risk Assessment	Not applicable	"National Security: A Propositional Study to Develop Resilience Indicators as an Aid to Personnel Vetting" (PDF)	2010	Academia	Personnel Vetting Practices	No	https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1003&context=asi
Organizational Resiliency and Risk Assessment	Not applicable	"A Review of Definitions and Measures of System Resilience" (PDF)	2016	Private sector	Not applicable	Yes	https://ideas.repec.org/a/eee/reensy/v145y2016icp47-61.html
Organizational Resiliency and Risk Assessment	Not applicable	"Concepts and Approaches to Resilience in a Variety of Governance and Regulatory Domains" (PDF)	2015	Academia	Not applicable	No	https://link.springer.com/article/10.1007/s10669-015-9553-6
Organizational Resiliency and Risk Assessment	Not applicable	"Does Gender Diversity Help Teams Constructively Manage Status Conflict? An Evolutionary Perspective of Status Conflict, Team Psychological Safety, and Team Creativity" (PDF)	2018	Academia	Not applicable	No	https://www.sciencedirect.com/science/article/pii/S0749597816302205
Organizational Resiliency and Risk Assessment	Not applicable	"Does Team Communication Represent a One-Size-Fits-All Approach? A Meta-Analysis of Team Communication and Performance" (PDF)	2018	Academia	Not applicable	No	https://www.sciencedirect.com/science/article/pii/S074959781630125X

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Organizational Resiliency and Risk Assessment	Not applicable	"Fostering Constructive Action by Peers and Bystanders in Organizations and Communities" (PDF)	2018	Academia	Not applicable	Yes	https://onlinelibrary.wiley.com/doi/full/10.1111/nejo.12221
Organizational Resiliency and Risk Assessment	Not applicable	"Risk Management Is Not Enough: A Conceptual Model for Resilience and Adaptation-Based Vulnerability Assessments" (PDF)	2015	Academia	Asset Protection	Yes	https://link.springer.com/article/10.1007/s10669-015-9552-7
Fraud Detection	Not applicable	"What You Can Learn About Fraud Prevention from a Casino: An Internal Auditor at Caesars Palace Shares the House's Tips for Detecting and Combating Fraud" (PDF)	2014	Private sector	Asset Protection	No	https://www.aicpastore.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2014/FVSNews/fromacasino.jsp
Fraud Detection	Not applicable	"Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries" (PDF)	2013	Academia	Insider Threats Asset Protection	No	https://dash.harvard.edu/bitstream/handle/1/10861136/Preventing%20Insider%20Theft-V%2041_3.pdf
Fraud Detection	Not applicable	"Anti Fraud Detection System" (HTML, plain text)	Undated	Private sector	Asset Protection	No	http://casinossecurity.com/anti-fraud-detection.htm
Fraud Detection	Not applicable	<i>Fraud Risk Management Guide: Executive Summary</i> (PDF)	2016	Private sector	Asset Protection	No	https://www.coso.org/Documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Fraud Detection	Not applicable	"The All-Pervasiveness of the Blockchain Technology" (PDF)	2018	Academia	Asset Protection	No	https://www.sciencedirect.com/science/article/pii/S1877050918300206
Fraud Detection	Not applicable	"5 Keys to Successfully Applying Machine Learning and AI and in Enterprise Fraud Detection" (HTML, plain text)	2018	Private sector	Asset Protection	No	https://www.fico.com/en/resource-download-file/4540
Fraud Detection	Not applicable	<i>Threat and Fraud Intelligence, Las Vegas Style</i> (PDF)	2006	Private sector	Asset Protection	No	https://jeffjonas.typepad.com/IEEE.Identity.resolution.pdf
Fraud Detection	Not applicable	"On the Hunt for Payroll Fraud: Taking a Close Look at Payroll Risks Can Enable Internal Auditors to Help Their Organizations Save Money and Identify Wrongdoing" (PDF)	2016	Private sector	Asset Protection	No	http://go.galegroup.com/ps/anonymous?id=GALE%7CA450695662&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00205745&p=AONE&sw=w
Fraud Detection	Not applicable	"Casino Gambling and Workplace Fraud: A Cautionary Tale for Managers" (PDF)	2010	Private sector	Asset Protection	No	https://www.emerald.com/insight/content/doi/10.1108/01409171011030381/full/html
Fraud Detection	Not applicable	"Intelligent Financial Fraud Detection Practices: An Investigation" (PDF)	2014	Academia	Asset Protection	No	https://arxiv.org/pdf/1510.07165.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Credentialing	Not applicable	<i>Review of Coast Guard's Oversight of the TWIC Program</i> (PDF)	2018	Government	Asset Protection	No	https://www.oig.dhs.gov/sites/default/files/assets/2018-10/OIG-18-88-Sep18.pdf
Credentialing	Not applicable	<i>Followup Audit: Navy Access Control Still Needs Improvement</i> (PDF)	2015	Government	Asset Protection	No	https://www.dodig.mil/reports.html/Article/1119227/followup-audit-navy-access-control-still-needs-improvement-redacted/
Credentialing	Not applicable	<i>DoD Needs to Improve Screening and Access Controls for General Public Tenants Leasing Housing on Military Installations</i> (PDF)	2016	Government	Personnel Vetting Practices	No	https://media.defense.gov/2016/Sep/22/200174203/-1/-1/1/DODIG-2016-072.pdf
Credentialing	Not applicable	<i>TWIC Background Checks Are Not as Reliable as They Could Be</i> (PDF)	2016	Government	Asset Protection	No	https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-128-Sep16.pdf
Credentialing	Not applicable	"Memorandum for Heads of Departments and Agencies, Chief Human Capital Officers, and Agency Security Officers: Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide" (PDF)	2008	Government	Preinvestigation and Investigation Asset Protection	No	https://www.opm.gov/suitability/suitability-executive-agent/policy/decision-making-guide.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Credentialing	Not applicable	<i>Military Personnel: Performance Measures Needed to Determine How Well DoD's Credentialing Program Helps Servicemembers</i> (PDF)	2016	Government	Not applicable	No	https://www.gao.gov/products/GAO-17-133
Credentialing	Not applicable	<i>Production of Secure Credentials for the Department of State and U.S. Customs and Border Protection</i> (PDF)	2015	Government	Asset Protection	No	https://www.gao.gov/products/GAO-15-326R
Credentialing	Not applicable	<i>Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards</i> (PDF)	2011	Government	Asset Protection	No	https://www.gao.gov/products/GAO-11-751
Credentialing	Not applicable	<i>VA Health Care: Improved Oversight and Compliance Needed for Physician Credentialing and Privileging Processes</i> (PDF)	2010	Government	Personnel Vetting Practices Asset Protection	No	https://www.gao.gov/products/GAO-10-26
Information Sharing and Reciprocity	Not applicable	<i>Cleared DoD Employees at Risk—Report 1: Policy Options for Removing Barriers to Seeking Help</i> (PDF)	2002	Government	Continuous Monitoring and Continuous Evaluation	No	https://www.dhra.mil/Portals/52/Documents/perserec/mr01-02.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Information Sharing and Reciprocity	Not applicable	<i>Reciprocity of Personnel Security Clearance and Access Determinations</i> (PDF)	2018	Government	Not applicable	No	https://www.dni.gov/files/documents/ICPG/cleaned/CPG-704.4---Reciprocity-of-Personnel-Security-Clearance-and-Access-Determinations-6-Jun-2018.pdf
Information Sharing and Reciprocity	Not applicable	<i>Cleared DoD Employees at Risk—Report 2: A Study of Barriers to Seeking Help</i> (PDF)	2002	Government	Continuous Monitoring and Continuous Evaluation	No	https://www.dhra.mil/Portals/52/Documents/perserec/tr01-04.pdf
Information Sharing and Reciprocity	Not applicable	<i>Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community</i> (PDF, plain text, HTML)	2016	Government	Asset Protection	No	https://www.dhs.gov/publication/ci-threat-info-sharing-framework
Information Sharing and Reciprocity	Not applicable	<i>Access to Classified Information</i> (Executive Order 12968) (PDF)	2008	Government	Asset Protection	No	https://fas.org/spp/clinton/eo12968.html
Information Sharing and Reciprocity	Not applicable	<i>FATF Guidance: Private Sector Information Sharing</i> (PDF)	2017	Government	Not applicable	No	http://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf
Information Sharing and Reciprocity	Not applicable	<i>Security Clearance Reciprocity: National Standards and Best Practices to Expedite Clearance Transfers</i> (PDF)	2017	Private sector	Not applicable	No	https://www.insaonline.org/wp-content/uploads/2017/07/INSA-Security-Clearance-Reciprocity-July-2017.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Information Sharing and Reciprocity	Not applicable	<i>Reciprocity of Background Investigations and National Security Adjudications</i> (Security Executive Agent Directive 7) (PDF)	2018	Government	Not applicable	No	https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-7_BI_ReciprocityU.pdf
Information Sharing and Reciprocity	Not applicable	"Public Trust in Health Information Sharing: A Measure of System Trust" (PDF)	2018	Academia	Not applicable	Yes	https://onlinelibrary.wiley.com/doi/pdf/10.1111/1475-6773.12654
Information Sharing and Reciprocity	Not applicable	<i>Critical Infrastructure Protection</i> (Presidential Decision Directive/NSC-63) (plain text, HTML)	1998	Government	Asset Protection	No	https://fas.org/irp/offdocs/pdd/pdd-63.htm
Information Sharing and Reciprocity	Not applicable	Intelligence Reform and Terrorism Prevention Act of 2004 (PDF)	2004	Government	Personnel Vetting Practices Asset Protection	No	https://www.govinfo.gov/content/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf
Information Sharing and Reciprocity	Not applicable	<i>Transportation Security: DHS Efforts to Eliminate Redundant Background Check Investigations</i> (PDF)	2007	Government	Asset Protection	No	https://www.gao.gov/products/GAO-07-756
Information Sharing and Reciprocity	Not applicable	<i>Security Clearances: FBI Has Enhanced Its Process for State and Local Law Enforcement Officials</i> (PDF)	2004	Government	Not applicable	No	https://www.gao.gov/products/gao-04-596

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Information Sharing and Reciprocity	Not applicable	"Information Sharing for Infrastructure Risk Management, Barriers and Solutions" (HTML, plain text)	2009	Academia	Asset Protection	No	https://create.usc.edu/sites/default/files/publications/informationsharingforinfrastructure/riskmanagementbarriers_0.pdf
Five Eyes Partner Practices	United Kingdom	Centre for the Protection of National Infrastructure (website)	Undated	Government (Foreign)	Asset Protection	No	https://www.cpmi.gov.uk
Five Eyes Partner Practices	United Kingdom	<i>Government Security: Roles and Responsibilities</i> (PDF)	2018	Government (Foreign)	Not applicable	No	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/758358/20180919_GovernmentSecurityRolesAndResponsibilities.pdf
Five Eyes Partner Practices	United Kingdom	<i>HMG Baseline Personnel Security Standard: Guidance on the Pre-Employment Screening of Civil Servants, Members of the Armed Forces, Temporary Staff and Government Contractors</i> (PDF)	2018	Government (Foreign)	Personnel Vetting Practices	No	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf
Five Eyes Partner Practices	United Kingdom	<i>HMG Personnel Security Controls</i> (PDF)	2018	Government (Foreign)	Personnel Vetting Practices Credentialing	No	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714017/HMG_Personnel_Security_Controls_-_May_2018.pdf

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Five Eyes Partner Practices	United Kingdom	Guidance on Departmental Information Risk Policy (PDF)	2013	Government (Foreign)	Asset Protection	No	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/365968/Guidance_on_Departmental_Information_Risk_Policy_v1_1_Apr-13.pdf
Five Eyes Partner Practices	United Kingdom	"Guidance: United Kingdom Security Vetting" (website)	2018	Government (Foreign)	Not applicable	No	https://www.gov.uk/guidance/security-vetting-and-clearance
Five Eyes Partner Practices	Australia	"Fact Sheets and Forms" (Website)	Undated	Government (Foreign)	Not applicable	No	http://www.defence.gov.au/AGSVA/factsheets-forms.asp
Five Eyes Partner Practices	Australia	"Corporate/Defence Industry Information and Policy" (website)	2019	Government (Foreign)	Organizational Resiliency and Risk Assessment	No	http://www.defence.gov.au/AGSVA/corporate-industry-policy.asp
Five Eyes Partner Practices	Australia	<i>Mitigating Insider Threats Through Personnel Security: Across Entities</i> (PDF)	2018	Government (Foreign)	Insider Threats	No	https://www.anao.gov.au/sites/g/files/het5496/ff/ANAO_Report_2017-2018_38.pdf
Five Eyes Partner Practices	Australia	<i>Central Administration of Security Vetting</i> (website)	2015	Government (Foreign)	Personnel Vetting Practices	No	https://www.anao.gov.au/work/performance-audit/central-administration-security-vetting

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Five Eyes Partner Practices	Australia	<i>Inquiry into Allegations of Inappropriate Vetting Practices in the Defence Security Authority and Related Matters, Inspector General of Intelligence and Security</i> (PDF)	2011	Government (Foreign)	Adjudication and Adjudication Bias	No	https://www.igis.gov.au/sites/default/files/files/Inquiries/docs/DSA_report.pdf
	New Zealand	<i>Overview of the Protective Security Requirements</i> (website)	2018	Government (Foreign)	Asset Protection	No	https://www.protectivesecurity.govt.nz/about-the-psr/overview/
	New Zealand	<i>NZIS 2016 Annual Report</i> (PDF)	2016	Government (Foreign)	Not applicable	No	https://www.nzsis.govt.nz/assets/media/nzsis-ar16.pdf
Five Eyes Partner Practices	New Zealand	<i>2017 Annual Report</i> (PDF)	2017	Government (Foreign)	Not applicable	No	https://www.nzsis.govt.nz/assets/media/nzsis-ar17.pdf
Five Eyes Partner Practices	New Zealand	<i>Inquiry into Security Clearance Vetting Processes</i> (PDF)	2010	Government (Foreign)	Adjudication and Adjudication Bias	No	Not available
Five Eyes Partner Practices	Canada	<i>Site Access Security Clearance for High-Security Sites</i> (PDF)	2012	Government (Foreign)	Asset Protection	No	http://nuclearsafety.gc.ca/eng/pdfs/Draft-RD-GD/DRAFT-RDGD-384-Site-Access-Security-Clearance-for-High-Security-Sites_e.pdf
Five Eyes Partner Practices	Canada	"Apply for Security Screening for Your Personnel" (website)	2018	Government (Foreign)	Personnel Vetting Practices	No	https://www.tpsgc-pwgsc.gc.ca/esc-src/personnel/enquete-screening-eng.html

Table A.1—Continued

Primary Category (Chapter)	Section	Title (Format)	Publication Year	Source (e.g., government, academia)	Related Chapter or Section	Fee?	URL
Five Eyes Partner Practices	Canada	"Audit of Personnel Security" (HTML, plain text)	2016	Government (Foreign)	Continuous Monitoring and Continuous Evaluation	No	http://www.rcmp-grc.gc.ca/en/audit-personnel-security
Five Eyes Partner Practices	Canada	<i>Broader Horizons: Preparing the Groundwork for Change in Security Intelligence Review</i> (HTML, plain text)	2015	Government (Foreign)	Not applicable	No	http://www.sirc-csars.gc.ca/anrran/2014-2015/index-eng.html

U.S. Policy and Law Relevant for Categories

This appendix lists relevant U.S. policies, orders, legal statutes, and guidance that pertain to categories in this annotated bibliography. For each entry, Table B.1 indicates the policy, guidance, or legislative reference; title; most applicable bibliography category or section; year; and the URL for source access.

Table B.1
Relevant U.S. Policy and Law

Policy, Guidance, or Legislative Reference	Title	Category/Section Applicability	Year	URL
32 C.F.R. § 147.2	Adjudicative Process	Adjudication and Adjudication Bias	As of 2019	https://www.law.cornell.edu/cfr/text/32/147.2
41 C.F.R. § 60-1.4	Equal Opportunity Clause	Suitability, Fitness, and Contractor Vetting	As of 2019	https://www.law.cornell.edu/cfr/text/41/60-1.4
49 C.F.R. § 1572.19	Applicant Responsibilities for a TWIC Security Threat Assessment	Credentialing	As of 2019	https://www.law.cornell.edu/cfr/text/49/1572.19
50 U.S.C. § 3341	Security Clearances	Preinvestigation and Investigation	As of 2019	https://www.law.cornell.edu/uscode/text/50/3341
C.F.R. §731.101	Purpose	Suitability, Fitness, and Contractor Vetting	As of 2019	https://www.law.cornell.edu/cfr/text/5/731.101
C.F.R. §731.202	Criteria for Making Suitability Determinations	Suitability, Fitness, and Contractor Vetting	As of 2019	https://www.law.cornell.edu/cfr/text/5/731.202
Pub. L. 95-454	Civil Service Reform Act of 1978	Preinvestigation and Investigation	1978	https://www.hsdl.org/?abstract&did=442377
DHS Instruction Handbook 121-01-007	<i>The Department of Homeland Security Personnel Suitability and Security Program</i>	Suitability, Fitness, and Contractor Vetting	2009	https://www.hsdl.org/?abstract&did=721598
DoD Directive 5210.42	<i>DoD Nuclear Weapons Personnel Reliability Assurance</i>	Suitability, Fitness, and Contractor Vetting	2012	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/521042p.pdf
DoD Instruction 1000.13	<i>Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals</i>	Credentialing	2014	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/100013p.pdf
DoD Instruction 5200.46	<i>DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)</i>	Credentialing	2014	https://www.cac.mil/Portals/53/Documents/520046p.pdf

Table B.1—Continued

Policy, Guidance, or Legislative Reference	Title	Category/Section	Applicability	Year	URL
DoD Manual 5200.02	<i>Procedures for the DoD Personnel Security Program (PSP)</i>	Insider Threats		2017	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520002_dodm_2017.pdf
DoD Directive 5240.06	<i>Counterintelligence Awareness and Reporting (CIAR)</i>	Insider Threats		2011	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/524006p.pdf
Executive Order 11246	<i>Equal Employment Opportunity</i>	Suitability, Fitness, and Contractor Vetting		1995	https://www.dol.gov/ofccp/regs/statutes/eo11246.htm
Executive Order 10450	<i>Security Requirements for Government Employment</i>	Preinvestigation and Investigation		1953	https://www.archives.gov/federal-register/codification/executive-order/10450.html
Executive Order 12333	<i>United States Intelligence Activities</i>	Insider Threats		1981	https://www.archives.gov/federal-register/codification/executive-order/12333.html
Executive Order 12829	<i>National Industrial Security Program</i>	Insider Threats		1993	https://www.govinfo.gov/content/pkg/WCPD-1993-01-11/pdf/WCPD-1993-01-11-Pg17.pdf
Executive Order 12968	<i>Access to Classified Information</i>	Preinvestigation and Investigation		2008	https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12968
Executive Order 13231	<i>Critical Infrastructure Protection in the Information Age</i>	Insider Threats		2001	https://www.hsdl.org/?abstract&did=620
Executive Order 13467	<i>Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information</i>	Preinvestigation and Investigation Suitability, Fitness, and Contractor Vetting		2008	https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-13467

Table B.1—Continued

Policy, Guidance, or Legislative Reference	Title	Category/Section Applicability	Year	URL
Executive Order 13764 (amending Executive Orders 13488 and 13467)	<i>To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters</i>	Suitability, Fitness, and Contractor Vetting	2017	https://obamawhitehouse.archives.gov/the-press-office/2017/01/17/amending-civil-service-rules-executive-order-13488-and-executive-order
Executive Order 13488	<i>Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust</i>	Information Sharing and Reciprocity	2009	https://www.hsdl.org/?abstract&did=799536
Executive Order 13526	<i>Classified National Security Information</i>	Preinvestigation and Investigation	2009	https://www.archives.gov/isoo/policy-documents/cnsi-eo.html
Executive Order 13549	<i>Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities</i>	Insider Threats	2010	https://obamawhitehouse.archives.gov/the-press-office/2010/08/18/executive-order-13549-classified-national-security-information-programs
Executive Order 13587	<i>Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information</i>	Information Sharing and Reciprocity	2011	https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net
Executive Order 13764	<i>Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters</i>	Preinvestigation and Investigation	2017	https://www.gpo.gov/fdsys/pkg/FR-2017-01-23/pdf/2017-01623.pdf

Table B.1—Continued

Policy, Guidance, or Legislative Reference	Title	Category/Section Applicability	Year	URL
Executive Order 13869	<i>Executive Order on Transferring Responsibility for Background Investigations to the Department of Defense</i>	Preinvestigation and Investigation Suitability, Fitness, and Contractor Vetting Continuous Monitoring and Continuous Evaluation	2019	https://www.whitehouse.gov/presidential-actions/executive-order-transferring-responsibility-background-investigations-department-defense/
Federal Investigations Notice 15-03	<i>Implementation of Federal Investigative Standards for Tier 1 and Tier 2 Investigations</i>	Preinvestigation and Investigation	2014	https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/2015/fin-15-03.pdf
Federal Investigations Notice 16-02	<i>Federal Investigative Standards for Tier 3 and Tier 3 Reinvestigation</i>	Preinvestigation and Investigation	2015	https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/2016/fin-16-02.pdf
Federal Investigations Notice 16-07	<i>Implementation of Federal Investigative Standards for Tier 4, Tier 4 Reinvestigation, Tier 5, and Tier 5 Reinvestigation</i>	Preinvestigation and Investigation	2016	https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/2016/fin-16-07.pdf
Federal Information Processing Standard 201-2	<i>Personal Identity Verification (PIV) of Federal Employees and Contractors</i>	Credentialing	2013	https://csrc.nist.gov/publications/detail/fips/201/2/final
HRM 9302.1	<i>Employment in the Excepted Service</i>	Preinvestigation and Investigation	2016	https://www.gsa.gov/directives-library/employment-in-the-excepted-service-93021-hrm
Homeland Security Presidential Directive 12	<i>Policy for a Common Identification Standard for Federal Employees and Contractors</i>	Credentialing	2004	https://www.dhs.gov/homeland-security-presidential-directive-12
Intelligence Community Directive 704	<i>Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information</i>	Preinvestigation and Investigation	2008	https://www.dni.gov/files/documents/ICD/ICD_704.pdf

Table B.1—Continued

Policy, Guidance, or Legislative Reference	Title	Category/Section	Applicability	Year	URL
Intelligence Community Directive 709	<i>Reciprocity for IC Employee Mobility</i>	Information Sharing and Reciprocity		2009	https://www.dni.gov/files/documents/ICD/ICD%20709.pdf
Intelligence Community Directive 503	<i>Information Technology Systems Security, Risk Management, Certification and Accreditation</i>	Insider Threats		As of 2019	https://www.dni.gov/files/documents/ICD/ICD_503.pdf
Intelligence Community Directive 700	<i>Protection of National Intelligence</i>	Insider Threats		As of 2019	https://www.dni.gov/files/documents/ICD/ICD_700.pdf
Intelligence Community Directive 705	<i>Sensitive Compartmented Information Facilities</i>	Insider Threats		As of 2019	https://www.dni.gov/files/documents/ICD/ICD_705_SCIFs.pdf
Intelligence Community Policy Guidance 704.3	<i>Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes</i>	Adjudication and Adjudication Bias		2008	http://www.dni.gov/files/documents/ICPG/icpg_704_3.pdf
Intelligence Community Policy Guidance 704.4	<i>Reciprocity of Personnel Security Clearance and Access Determinations</i>	Information Sharing and Reciprocity		2008	https://www.dni.gov/files/documents/ICPG/icpg_704_4.pdf
Intelligence Community Policy Guidance 704.6	<i>Conduct of Polygraph Examinations for Personnel Security Vetting</i>	Preinvestigation and Investigation		2015	https://www.dni.gov/files/documents/ICPG/ICPG%20704.6.pdf
National Insider Threat Policy	<i>National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs</i>	Insider Threats		2012	https://www.dni.gov/index.php/ic-legal-reference-book/presidential-memorandum-nitp-minimum-standards-for-insider-threat-program
National Infrastructure Protection Plan 2013	<i>National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience</i>	Information Sharing and Reciprocity		2013	https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf
National Industrial Security Program Operating Manual (DoD 5220.22-M)	<i>Department of Defense National Industrial Security Program Operating Manual</i>	Suitability, Fitness, and Credentialing		2016	https://fas.org/sgp/library/nispom/nispom2006.pdf

Table B.1—Continued

Policy, Guidance, or Legislative Reference	Title	Category/Section Applicability	Year	URL
National Insider Threat Task Force memo	"Clarification of Enterprise Audit Management (EAM), User Activity Monitoring (UAM), Continuous Monitoring, and Continuous Evaluation"	Continuous Monitoring and Continuous Evaluation	2014	https://www.qmulos.com/wp-content/uploads/2016/11/EAM_UAM_and_Continuous_Monitoring_Definitions-Signed.pdf
National Security Directive 42	<i>National Policy for the Security of National Security Telecommunications and Information Systems</i>	Insider Threats	1990	https://www.hsdl.org/?abstract&did=458706
National Security Directive 63	<i>Single Scope Background Investigations</i>	Insider Threats	1991	https://fas.org/sgp/othergov/nsd63.html
National Security Presidential Directive 54/Homeland Security Presidential Directive 23	<i>Cybersecurity Policy</i>	Insider Threats	As of 2019	https://fas.org/irp/offdocs/nsdp/nsdpd-54.pdf
OPM memo	"Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12"	Credentialing	2008	https://www.opm.gov/investigations/suitability-executive-agent/policy/final-credentialing-standards.pdf
OMB memo	"Reciprocal Recognition of Existing Personnel Security Clearances"	Information Sharing and Reciprocity	2006	https://www.cdse.edu/toolkits/personnel/policy.html
PDD/NSC-12	<i>Security Awareness and Reporting of Foreign Contacts</i>	Insider Threats	1993	https://fas.org/irp/offdocs/pdd12.htm
Presidential Policy Directive 21	<i>Critical Infrastructure Security and Resilience</i>	Insider Threats	As of 2019	https://www.dhs.gov/taxonomy/term/2586/all/feed
Pub. L. 113-66	National Defense Authorization Act for Fiscal Year 2014	Information Sharing and Reciprocity	2014	https://www.congress.gov/bill/113th-congress/house-bill/3304/text
Pub. L. 108-458	Intelligence Reform and Terrorism Prevention Act	Information Sharing and Reciprocity	2004	https://www.dni.gov/index.php/who-we-are/organizations/ogc/ogc-related-menus/ogc-related-content/irtpa-of-2004

Table B.1—Continued

Policy, Guidance, or Legislative Reference	Title	Category/Section Applicability	Year	URL
Pub. L. 115-173	Securely Expediting Clearances Through Reporting Transparency Act of 2018	Preinvestigation and Investigation	2018	https://www.congress.gov/bill/115th-congress/house-bill/3210?q=%7B%22search%22%3A%5B%22secret+act%22%5D%7D&r=3
Security Executive Agent Directive 1	<i>Security Executive Agent Authorities and Responsibilities</i>	Preinvestigation and Investigation	2012	https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-policy_
Security Executive Agent Directive 2	<i>Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position</i>	Preinvestigation and Investigation	2014	https://www.dni.gov/files/NCSC/documents/Regulations/Security-Executive-Agent-Directive-2-September-2014.pdf
Security Executive Agent Directive 3	<i>Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position</i>	Preinvestigation and Investigation	2017	https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf
Security Executive Agent Directive 4	<i>National Adjudicative Guidelines</i>	Adjudication and Adjudication Bias	2017	https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf
Security Executive Agent Directive 5	<i>Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications</i>	Preinvestigation and Investigation	2016	https://www.dni.gov/files/NCSC/documents/Regulations/SEAD_5.pdf
Security Executive Agent Directive 6	<i>Continuous Evaluation</i>	Continuous Monitoring and Continuous Evaluation	2018	https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-6-continuous%20evaluation-U.pdf
Security Executive Agent Directive 7	<i>Reciprocity of Background Investigations and National Security Adjudications</i>	Information Sharing and Reciprocity	2018	https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-7_Bl_ReciprocityU.pdf

Table B.1—Continued

Policy, Guidance, or Legislative Reference	Title	Category/Section	Applicability	Year	URL
18 U.S.C. § 2510	Definitions	Insider Threats		1986	https://www.law.cornell.edu/uscode/text/18/2510
18 U.S.C. § 2701	Unlawful Access to Stored Communications	Insider Threats		As of 2019	https://www.law.cornell.edu/uscode/text/18/2701
28 U.S.C. § 535	Investigation of Crimes Involving Government Officers and Employees; Limitations	Insider Threats		As of 2019	https://www.law.cornell.edu/uscode/text/28/535
32 C.F.R. Part 147, Subpart B	Investigative Standards	Insider Threats		As of 2019	https://www.law.cornell.edu/cfr/text/32/part-147
32 C.F.R. Part 2001	Classified National Security Information	Insider Threats		As of 2019	https://www.law.cornell.edu/cfr/text/32/part-2001
41 C.F.R. Part 102-74	Facility Management; Subpart C, Conduct on Federal Property	Insider Threats		As of 2019	https://www.law.cornell.edu/cfr/text/41/part-102-74
42 U.S.C. § 2000ee-3	Federal Agency Data Mining Reporting	Insider Threats		2007	https://www.law.cornell.edu/uscode/text/42/2000ee-3
44 U.S.C. § 3506	Federal Agency Responsibilities	Insider Threats		1995	https://www.law.cornell.edu/uscode/text/44/3506
44 U.S.C. § 3534	Federal Agency Responsibilities	Insider Threats		2002	https://www.law.cornell.edu/uscode/text/44/3534
44 U.S.C. § 3536	National Security Systems	Insider Threats		2002	https://www.law.cornell.edu/uscode/text/44/3536
44 U.S.C. § 3544	Federal Agency Responsibilities	Insider Threats		2002	https://www.law.cornell.edu/uscode/text/44/3544
44 U.S.C. § 3546	Federal Information Security Incident Center	Insider Threats		2002	https://www.law.cornell.edu/uscode/text/44/3546
44 U.S.C. § 3547	National Security Systems	Insider Threats		2002	https://www.law.cornell.edu/uscode/text/44/3547

Table B.1—Continued

Policy, Guidance, or Legislative Reference	Title	Category/Section	Applicability	Year	URL
5 U.S.C. § 1304	Loyalty Investigations; Reports; Revolving Fund	Insider Threats		As of 2019	https://www.law.cornell.edu/uscode/text/5/1304
5 U.S.C. § 3301	Civil Service; Generally	Insider Threats		As of 2019	https://www.law.cornell.edu/uscode/text/5/3301
5 U.S.C. § 3302	Competitive Service; Rules	Insider Threats		As of 2019	https://www.law.cornell.edu/uscode/text/5/3302
5 U.S.C. § 552A	Records Maintained on Individuals	Insider Threats		1974	https://www.law.cornell.edu/uscode/text/5/552a
5 U.S.C. § 7311	Loyalty and Striking	Insider Threats		As of 2019	https://www.law.cornell.edu/uscode/text/5/7311
5 U.S.C. § 7312	Employment and Clearance; Individuals Removed for National Security	Insider Threats		As of 2019	https://www.law.cornell.edu/uscode/text/5/7312
5 U.S.C. § 7313	Riots and Civil Disorders	Insider Threats		As of 2019	https://www.law.cornell.edu/uscode/text/5/7313
5 U.S.C. § 7532	Suspension and Removal	Insider Threats		As of 2019	https://www.law.cornell.edu/uscode/text/5/7532
5 U.S.C. § 9101	Access to Criminal History Records for National Security and Other Purposes	Insider Threats		As of 2019	https://www.law.cornell.edu/uscode/text/5/9101
5 C.F.R. Part 736	Personnel Investigations	Insider Threats		As of 2019	https://www.law.cornell.edu/cfr/text/5/part-736
50 U.S.C. § 402a	Coordination of Counterintelligence Matters	Insider Threats		2002	https://www.govinfo.gov/app/details/USCODE-2011-title50/USCODE-2011-title50-chap15-subchap1-sec402a
Under Secretary of Defense for Intelligence memorandum	“Notifications Required upon the Receipt or Development of Unresolved Criminal Conduct”	Suitability, Fitness, and Contractor Vetting		2013	https://www.cdse.edu/documents/toolkits-psa/Notification-Required-Upon-the-Receipt-or-Development-of-Unresolved-Criminal-Conduct.pdf

Boolean Search Terms and Strings

Database	Subdatabase	Search Terms
EBSCOhost	• Academic Search Complete • Business Source Complete • Criminal Justice Abstracts • Military and Government Collection • PsychINFO	((<i>"insider threat"</i> OR <i>"insider threats"</i>)) AND ((<i>vetting</i> OR <i>vetted</i> OR <i>behavioral</i> OR <i>behavioral</i> OR <i>psychological</i> OR <i>fraud*</i> OR <i>predict*</i> OR <i>mitigat*</i> OR <i>"industrial security"</i> OR <i>suitability</i> OR <i>indicators</i> OR <i>factors</i> OR <i>emerging</i> OR <i>credential*</i> OR <i>screening</i> OR <i>investigation*</i> OR <i>detect*</i> OR <i>barrier*</i> OR <i>"continuous evaluation"</i>)) su((<i>"security clearance"</i> OR <i>polygraph</i> OR <i>"lie detector"</i>)) AND noft((<i>"insider threat"</i> OR <i>"insider threats"</i> OR <i>vetting</i> OR <i>vetted</i> OR <i>behavioral</i> OR <i>behavioral</i> OR <i>psychological</i> OR <i>fraud*</i> OR <i>predict*</i> OR <i>mitigat*</i> OR <i>"industrial security"</i> OR <i>suitability</i> OR <i>indicators</i> OR <i>factors</i> OR <i>emerging</i> OR <i>credential*</i> OR <i>screening</i> OR <i>investigation*</i> OR <i>detect*</i> OR <i>barrier*</i> OR <i>"continuous evaluation"</i>))
ProQuest	• Military Database • Policy File Index • Public Affairs Index • Digital National Security Archive • PAIS Index	noft((<i>"insider threat"</i> OR <i>"insider threats"</i>)) AND ((<i>vetting</i> OR <i>vetted</i> OR <i>behavioral</i> OR <i>behavioral</i> OR <i>psychological</i> OR <i>fraud*</i> OR <i>predict*</i> OR <i>mitigat*</i> OR <i>"industrial security"</i> OR <i>suitability</i> OR <i>indicators</i> OR <i>factors</i> OR <i>emerging</i> OR <i>credential*</i> OR <i>screening</i> OR <i>investigation*</i> OR <i>detect*</i> OR <i>barrier*</i> OR <i>"continuous evaluation"</i>)) su((<i>"security clearance"</i> OR <i>polygraph</i> OR <i>"lie detector"</i>)) AND noft((<i>"insider threat"</i> OR <i>"insider threats"</i> OR <i>vetting</i> OR <i>vetted</i> OR <i>behavioral</i> OR <i>behavioral</i> OR <i>psychological</i> OR <i>fraud*</i> OR <i>predict*</i> OR <i>mitigat*</i> OR <i>"industrial security"</i> OR <i>suitability</i> OR <i>indicators</i> OR <i>factors</i> OR <i>emerging</i> OR <i>credential*</i> OR <i>screening</i> OR <i>investigation*</i> OR <i>detect*</i> OR <i>barrier*</i> OR <i>"continuous evaluation"</i>))
Nexis Uni	• Searches of newspaper articles in FVEY countries	hlead((<i>"insider threat"</i> OR <i>"insider threats"</i>)) AND hlead((<i>vetting</i> OR <i>vetted</i> OR <i>behavioral</i> OR <i>behavioral</i> OR <i>psychological</i> OR <i>fraud*</i> OR <i>predict*</i> OR <i>mitigat*</i> OR <i>"industrial security"</i> OR <i>suitability</i> OR <i>indicators</i> OR <i>factors</i> OR <i>emerging</i> OR <i>credential*</i> OR <i>screening</i> OR <i>investigation*</i> OR <i>detect*</i> OR <i>barrier*</i> OR <i>"continuous evaluation"</i>))

References

Astakhova, L. V., "Evaluation Assurance Levels for Human Resource Security of an Information System," *Procedia Engineering*, Vol. 129, 2015, pp. 635–639.

Australian Attorney-General's Department, "The Protective Security Policy Framework," webpage, undated. As of August 13, 2019:
<https://www.protectivesecurity.gov.au/Pages/default.aspx>

———, *Protective Security Policy Framework: 2016–2017 Compliance Report*, Canberra, 2017.

Australian Department of Defence, "Australian Government Security Vetting FAQ," webpage, undated. As of August 19, 2019:
<http://www.defence.gov.au/AGSVA/FAQ/clearance-subject.asp>

Australian National Audit Office, *Central Administration of Security Vetting*, Canberra, June 9, 2015. As of February 21, 2019:
<https://www.anao.gov.au/work/performance-audit/central-administration-security-vetting>

Berkelaar, Brenda L., *Cyber-Vetting: Exploring the Implications of Online Information for Career Capital and Human Capital Decisions*, dissertation, West Lafayette, Ind.: Purdue University, 2010.

Bui, Lynh, Dan Lamothe, and Michael E. Miller, "Coast Guard Lieutenant Used Work Computers in Alleged Planning of Widespread Domestic Terrorist Attack, Prosecutors Say," *Washington Post*, February 21, 2019. As of August 6, 2019:
https://www.washingtonpost.com/local/public-safety/ex-coast-guard-lieutenant-ordered-held-for-14-days-while-government-weighs-terrorism-related-charges-in-his-planning-of-widespread-terrorist-attack/2019/02/21/57918f12-3573-11e9-854a-7a14d7fec96a_story.html

Code of Federal Regulations, Title 5, Administrative Personnel; Chapter I, Office of Personnel Management; Subchapter A, Civil Service Rules; Part 1, Coverage and Definitions (Rule I); Section 1.1, Positions and Employees Affected by the Rules in this Subchapter, January 1, 2008. As of July 29, 2019:
<https://www.govinfo.gov/app/details/CFR-2008-title5-vol1/CFR-2008-title5-vol1-sec1-1>

———, Title 5, Administrative Personnel; Chapter I, Office of Personnel Management; Subchapter A, Civil Service Rules; Part 2, Appointment Through the Competitive Service; Related Matters (Rule II); Section 2.1, Competitive Examinations and Eligible Registers; Suitability and Fitness for Civil Service Employment, January 1, 2019. As of July 30, 2019:
<https://www.govinfo.gov/app/details/CFR-2019-title5-vol1/CFR-2019-title5-vol1-sec2-1>

———, Title 5, Administrative Personnel; Chapter I, Office of Personnel Management; Subchapter A, Civil Service Rules; Part 5, Regulations, Investigation, and Enforcement (Rule V); Section 5.2, Investigation and Evaluations, January 1, 2019. As of July 30, 2019:
<https://www.govinfo.gov/app/details/CFR-2019-title5-vol1/CFR-2019-title5-vol1-sec5-2>

———, Title 5, Administrative Personnel; Chapter XVI, Office of Government Ethics; Subchapter B, Government Ethics; Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch. As of July 25, 2019:

<https://www.govinfo.gov/content/pkg/CFR-2011-title5-vol1/pdf/CFR-2011-title5-vol1-chapI.pdf>

———, Title 5, Administrative Personnel; Chapter XVI, Office of Government Ethics; Subchapter B, Government Ethics; Part 731, Sustainability. As of July 25, 2019:

<https://www.govinfo.gov/content/pkg/CFR-2011-title5-vol1/pdf/CFR-2011-title5-vol1-chapI.pdf>

———, Title 32, National Defense; Subtitle A, Department of Defense; Chapter I, Office of the Secretary of Defense; Subchapter D, Personnel, Military and Civilian; Part 147, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information. As of July 30, 2019: <https://www.govinfo.gov/content/pkg/CFR-2012-title32-vol1/xml/CFR-2012-title32-vol1-part147.xml>

Cronk, Terri Moon, “DoD Unveils Its Artificial Intelligence Strategy,” U.S. Department of Defense, February 12, 2019. As of July 25, 2019:

<https://dod.defense.gov/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/>

Department of Defense Directive 5210.48, *Credibility Assessment (CA) Program*, Washington, D.C.: April 24, 2015, incorporating change 1, effective February 12, 2018. As of August 20, 2019:

https://fas.org/irp/doddir/dod/d5210_48.pdf

Department of Defense Instruction 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, Washington, D.C.: U.S. Department of Defense, January 23, 2014, incorporating change 1, December 14, 2017. As of August 12, 2019:

<https://www.cac.mil/Portals/53/Documents/DODI-1000.13.pdf>

Department of Defense Manual 1000.13, *DoD Identification (ID) Cards: ID Card Life-Cycle*, Vol. 1, Washington, D.C.: U.S. Department of Defense, January 23, 2014. As of August 12, 2019:

https://www.cac.mil/Portals/53/Documents/DODM-1000.13_vol1.pdf

Department of Defense Manual 1000.13, Vol. 2, *DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, Vol. 2, Washington, D.C.: U.S. Department of Defense, January 23, 2014. As of August 12, 2019:

https://www.cac.mil/Portals/53/Documents/DODM-1000.13_vol2.pdf

Department of the Navy v. Egan, 484 U.S. 518, 1988.

DHS—See U.S. Department of Homeland Security.

DoD—See Department of Defense.

Dunbar, Brian, “Statement for the Record for Brian Dunbar, Assistant Director, Special Security Directorate, National Counterintelligence and Security Center, testimony before the Senate Select Committee on Intelligence Hearing on Security Clearance Reform,” March 7, 2018.

El-Ganayni v. United States DOE, 2008 U.S. Dist., W.D. Pa., 2010.

European Programme for Critical Infrastructure Protection, “Critical Infrastructure,” webpage, undated. As of August 22, 2019:

https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

Executive Order 10450, *Security Requirements for Government Employment*, Washington, D.C.: White House, April 27, 1953. As of July 25, 2019:

<https://www.archives.gov/federal-register/codification/executive-order/10450.html>

Executive Order 10577, *Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service*, Washington, D.C.: White House, November 23, 1954. As of July 25, 2019:

<https://www.archives.gov/federal-register/codification/executive-order/10577.html>

Executive Order 12829, *National Industrial Security Program*, Washington, D.C.: White House, January 6, 1993. As of August 5, 2019:

<https://www.govinfo.gov/content/pkg/WCPD-1993-01-11/pdf/WCPD-1993-01-11-Pg17.pdf>

Executive Order 12968, *Access to Classified Information*, Washington, D.C.: White House, August 2, 1995. As of July 25, 2019:

<https://fas.org/sgp/clinton/eo12968.html>

Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, Washington, D.C.: White House, June 30, 2008. As of July 30, 2019:

<https://fas.org/irp/offdocs/eo/eo-13467.htm>

Executive Order 13488, *Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust*, Washington, D.C.: White House, January 16, 2009. As of July 30, 2019:

<https://www.govinfo.gov/content/pkg/WCPD-2009-01-19/pdf/WCPD-2009-01-19-Pg87.pdf>

Executive Order 13526, *Classified National Security Information*, Washington, D.C.: White House, December 29, 2009. As of August 5, 2019:

<https://www.govinfo.gov/content/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-eo13526.pdf>

Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, Washington, D.C.: White House, October 7, 2011. As of August 5, 2019:

<https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/>

executive-order-13587-structural-reforms-improve-security-classified-net

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, Washington, D.C.: White House, February 12, 2013. As of August 9, 2019:

<https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/>

executive-order-improving-critical-infrastructure-cybersecurity

Executive Order 13869, *Transferring Responsibility for Background Investigations to the Department of Defense*, Washington, D.C.: White House, April 24, 2019. As of July 25, 2019:

<https://www.whitehouse.gov/presidential-actions/>

executive-order-transferring-responsibility-background-investigations-department-defense/

Executive Order 13859, *Maintaining American Leadership in Artificial Intelligence*, Washington, D.C.: White House, February 11, 2019. As of July 25, 2019:

<https://www.whitehouse.gov/presidential-actions/>

executive-order-maintaining-american-leadership-artificial-intelligence/

FitzHarris, J. B., I. Jacoby, S. B. Permison, and P. McCardle, "Challenges of Including Dietitians, Nurses, Occupational Therapists, and Pharmacists in the Federal Credentialing Program," *Military Medicine*, Vol. 165, No. 10, 2000, pp. 716–720.

GAO—See U.S. Government Accountability Office.

Girardin, Lauren, "Can Trusted Workforce 2.0 Fix Government's Security Clearance Woes?"

GovLoop.com, April 2, 2018. As of August 22, 2019:

<https://www.govloop.com/community/blog/>

can-trusted-workforce-2-0-fix-governments-security-clearance-woes/

Government of Canada, *National Strategy for Critical Infrastructure*, Ottawa, 2009. As of August 22, 2019:

<https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf>

———, “Government Security Screening,” webpage, updated July 18, 2018. As of February 4, 2019: <https://www.canada.ca/en/security-intelligence-service/services/government-security-screening.html>

Greene v. McElroy, 360 U.S. 474, 1959.

Griswold v. Connecticut, 381 U.S. 479, 1965.

Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, Washington, D.C.: U.S. Department of Homeland Security, August 27, 2014.

Horton, Alex, “Immigrant Recruits Face More Scrutiny Than White Supremacists When They Enlist,” *Washington Post*, February 21, 2019. As of August 6, 2019:

<https://www.washingtonpost.com/national-security/2019/02/21/immigrant-recruits-face-more-scrutiny-than-white-supremacists-when-they-enlist-heres-why/>

Hunker, Jeffrey, and Christian W. Probst, “Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, Vol. 2, No. 1, 2011, pp. 4–27.

Hunter, Fergus, “Alarm as Top-Level Security Vetting Is Being Outsourced to Private Contractors,” *Sydney Morning Herald*, September 3, 2018. As of July 25, 2019:

<https://www.smh.com.au/politics/federal/alarm-as-top-level-security-vetting-is-outsourced-to-private-contractors-20180831-p500yy.html>

Intelligence and National Security Alliance, *A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector*, Arlington, Va., September 2013. As of August 22, 2019:

<https://www.insaonline.org/a-preliminary-examination-of-insider-threat-programs-in-the-u-s-private-sector/>

———, *Leveraging Emerging Technologies in the Security Clearance Process*, Arlington, Va., March 2014. As of August 22, 2019:

https://www.insaonline.org/wp-content/uploads/2017/04/INSA_LeveragingEmergingTech_WP.pdf

Intelligence Community Policy Guidance 704.2, *Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*, Washington, D.C.: Office of the Director of National Intelligence, October 2, 2008.

Keeney, M., E. Kowalski, D. Cappelli, A. Moore, T. Shimeall, and S. Rogers, *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, Pittsburgh, Pa.: Carnegie Mellon Software Engineering Institute, 2005. As of July 25, 2019:

https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf

Makky v. Chertoff, 541 F.3d 205, 3d Cir., 2008.

Nan, L., and D. Biros, “Identifying Common Characteristics of Malicious Insiders,” *Proceedings of the Conference on Digital Forensics, Security and Law*, 2015, pp. 161–175.

NASA v. Nelson, 562 U.S. 134, 2011.

National Institute of Standards and Technology, Computer Security Resource Center, *Glossary*, Gaithersburg, Md., undated. As of July 25, 2019:

<https://csrc.nist.gov/glossary/term/information-security-continuous-monitoring>

ODNI—See Office of the Director of National Intelligence.

Office of Inspector General, Office of Audits, NASA, *Audit of NASA's Information Technology Supply Chain Risk Management Efforts*, Washington, D.C., IG-18-019 (A-17-008-00), May 24, 2018. As of August 12, 2019:

<https://oig.nasa.gov/docs/IG-18-019.pdf>

Office of Management and Budget, "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," memorandum, Washington, D.C., April 21, 2010.

Office of the Director of National Intelligence, "Continuous Evaluation—Overview," webpage, undated. As of March 1, 2019:

<https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-continuous-evaluation-overview>

———, "Continuous Evaluation: Top 15 Frequently Asked Questions," April 3, 2017. As of July 25, 2019:

<https://www.dni.gov/files/NCSC/documents/products/20180316-CE-FAQs.pdf>

Office of the Inspector General, U.S. Department of Defense, *The Missile Defense Agency Can Improve Supply Chain Security for the Ground-Based Midcourse Defense System*, redacted version, Washington, D.C., DODIG-2017-076, April 27, 2017. As of August 12, 2019:

<https://media.defense.gov/2017/Dec/19/2001858398/-1/-1/1/DODIG-2017-076-REDACTED.PDF>

Office of Personnel Management, "Suitability Executive Agent: Position Designation Tool," webpage, undated. As of August 13, 2019:

<https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/>

OMB—*See* Office of Management and Budget.

OPM—*See* Office of Personnel Management.

Perez v. FBI, 714 F. Supp. 1414, W.D. Tex. 1989.

Presidential Policy Directive 8, *National Preparedness*, Washington, D.C.: White House, March 30, 2011. As of August 9, 2019:

<https://www.hsdl.org/?abstract&did=7423>

Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, Washington, D.C.: White House, February 12, 2013. As of August 9, 2019:

<https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

President's Management Agenda, *Security Clearance, Suitability/Fitness, and Credentialing Reform*, Washington, D.C., 2018. As of July 25, 2019:

https://www.performance.gov/CAP/action_plans/FY2018_Q2_Security_Suitability.pdf

Protective Security Requirements, homepage, undated. As of January 30, 2018:

<https://www.protectivesecurity.govt.nz/>

Public Law 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, October 26, 2001. As of July 29, 2019:

<https://www.govinfo.gov/app/details/PLAW-107publ56>

Public Law 107-295, Maritime Transportation Security Act of 2002, Section 102, November 25, 2002. As of August 12, 2019:

<https://www.govinfo.gov/app/details/PLAW-107publ295>

Public Law 107-347, E-Government Act of 2002, December 17, 2002. As of July 29, 2019:

<https://www.govinfo.gov/app/details/PLAW-107publ347>

Public Law 108-458, Intelligence Reform and Terrorism Prevention Act of 2004, December 17, 2004. As of July 29, 2019:

<https://www.govinfo.gov/content/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf>

Tiwari v. Mattis, 363 F. Supp. 3d 1154, W.D. Wash., 2019.

UK Cabinet Office, *Data Handling Procedures in Government*, London, June 2008. As of August 19, 2019:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60966/final-report.pdf

———, *Government Transformation Strategy*, London, February 9, 2017. As of August 22, 2019: <https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy>

———, *HMG Baseline Personnel Security Standard*, London, updated May 2018. As of August 22, 2019:

<https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>

———, “Security Policy Framework, May 2018,” webpage, last updated May 24, 2018. As of August 13, 2019:

<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>

UK Ministry of Defence, “Guidance: United Kingdom Security Vetting,” webpage, last updated August 2, 2019. As of August 13, 2019:

<https://www.gov.uk/guidance/security-vetting-and-clearance>

United States v. Maynard, 615 F.3d 544, D.C. Cir., 2010.

U.S. Code, Title 5, Government Organization and Employees; Part III, Employees; Subpart B, Employment and Retention; Chapter 33, Examination, Selection, and Placement; Subchapter I, Examination, Certification, and Appointment; Section 3301, Civil Service. As of July 25, 2019: <https://www.govinfo.gov/app/details/USCODE-2011-title5/USCODE-2011-title5-partIII-subpartB-chap33>

U.S. Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*, Washington, D.C., 2009. As of August 22, 2019: https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

———, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, Washington, D.C., 2013.

U.S. Government Accountability Office, *VA Health Care: Improved Screening of Practitioners Would Reduce Risk to Veterans*, Washington, D.C., GAO-04-566, March 31, 2004. As of August 12, 2019: <https://www.gao.gov/products/GAO-04-566>

———, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, Washington, D.C., GAO-05-106, December 10, 2004. As of August 12, 2019: <https://www.gao.gov/products/GAO-05-106>

———, *Industrial Security: DOD Cannot Ensure Its Oversight of Contractors Under Foreign Influence Is Sufficient*, Washington, D.C., GAO-05-681, July 15, 2005. As of August 22, 2019: <https://www.gao.gov/new.items/d05681.pdf>

———, *Employee Security: Implementation of Identification Cards and DoD's Personnel Security Clearance Program Need Improvement*, Washington, D.C., GAO-08-551T, April 9, 2008. As of August 12, 2019: <https://www.gao.gov/products/GAO-08-551T>

Webster v. Doe, 486 U.S. 592, 1988.

White House, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, Washington, D.C., November 2012. As of August 5, 2019:
<https://fas.org/sgp/obama/insider.pdf>

———, *National Strategy for Information Sharing and Safeguarding*, Washington, D.C., 2012.

Whyte, Sally, “Vetting Agency Not Protecting Against Internal Threats: Audit Report,” *Sydney Morning Herald*, May 12, 2018. As of August 22, 2019:
[https://www.smh.com.au/politics/federal/](https://www.smh.com.au/politics/federal/vetting-agency-not-protecting-against-internal-threats-audit-report-20180511-p4zetr.html)
[vetting-agency-not-protecting-against-internal-threats-audit-report-20180511-p4zetr.html](https://www.smh.com.au/politics/federal/vetting-agency-not-protecting-against-internal-threats-audit-report-20180511-p4zetr.html)

———, “Hundreds of Waivers for Security Clearances Handed Out,” *Canberra Times*, October 9, 2018. As of July 25, 2019:
[https://www.canberratimes.com.au/story/6002116/](https://www.canberratimes.com.au/story/6002116/hundreds-of-waivers-for-security-clearances-handed-out/)
[hundreds-of-waivers-for-security-clearances-handed-out/](https://www.canberratimes.com.au/story/6002116/hundreds-of-waivers-for-security-clearances-handed-out/)

