



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**U.S. SECURITY CLEARANCES: REDUCING THE
SECURITY CLEARANCE BACKLOG WHILE
PRESERVING INFORMATION SECURITY**

by

Benjamin F. Berger

March 2019

Co-Advisors:

Robert L. Simeral
Erik J. Dahl

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 2019	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE U.S. SECURITY CLEARANCES: REDUCING THE SECURITY CLEARANCE BACKLOG WHILE PRESERVING INFORMATION SECURITY			5. FUNDING NUMBERS	
6. AUTHOR(S) Benjamin F. Berger				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) From 2014–2018, the U.S. federal government security clearance backlog increased from 190,000 investigations to 710,000 investigations, according to a 2018 Government Accountability Office report. The backlog of security clearance investigations has resulted in investigation timelines that range between 134 and 395 days. The organization that handles 90 percent of the caseload for background investigations, the National Background Investigations Bureau (NBIB), has the capability to provide approximately 160,000–180,000 investigations annually. With current staffing structure, the NBIB can handle approximately 25 percent of the security clearance caseload. Changes in policy could be considered to address this critical issue; however, drastic change may be required to adequately address this issue. This thesis recommends a transformational organizational change to the National Background Investigations Bureau to address the backlog of security clearance investigations. A policy change that limits the annual amount of security clearance investigations to the throughput of the NBIB would reduce the backlog of security clearance investigations, increase the quality of investigations, and increase the integrity of national security information without adding to the costs of security clearances.				
14. SUBJECT TERMS security clearance, risk management, information security			15. NUMBER OF PAGES 79	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**U.S. SECURITY CLEARANCES: REDUCING THE SECURITY CLEARANCE
BACKLOG WHILE PRESERVING INFORMATION SECURITY**

Benjamin F. Berger
Regional and Stakeholder Lead, Federal Emergency Management Agency,
Department of Homeland Security
BA, Virginia Commonwealth University, 2011

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
March 2019**

Approved by: Robert L. Simeral
Co-Advisor

Erik J. Dahl
Co-Advisor

Erik J. Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

From 2014–2018, the U.S. federal government security clearance backlog increased from 190,000 investigations to 710,000 investigations, according to a 2018 Government Accountability Office report. The backlog of security clearance investigations has resulted in investigation timelines that range between 134 and 395 days. The organization that handles 90 percent of the caseload for background investigations, the National Background Investigations Bureau (NBIB), has the capability to provide approximately 160,000–180,000 investigations annually. With current staffing structure, the NBIB can handle approximately 25 percent of the security clearance caseload. Changes in policy could be considered to address this critical issue; however, drastic change may be required to adequately address this issue. This thesis recommends a transformational organizational change to the National Background Investigations Bureau to address the backlog of security clearance investigations. A policy change that limits the annual amount of security clearance investigations to the throughput of the NBIB would reduce the backlog of security clearance investigations, increase the quality of investigations, and increase the integrity of national security information without adding to the costs of security clearances.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	THE SECURITY CLEARANCE BACKLOG—A HOMELAND SECURITY CHALLENGE	1
A.	BACKGROUND	1
B.	PROBLEM STATEMENT	2
C.	RESEARCH QUESTION	4
D.	LITERATURE REVIEW	4
	1. Information Security	4
	2. Personnel Security	5
	3. Risk Management	7
	4. Organizational Change.....	8
	5. Authorities	9
	6. Government Reports and Current Recommendations	10
	7. Summary.....	11
E.	RESEARCH DESIGN	12
	1. Object of Study.....	12
	2. Limitations and Scope	12
	3. Instrumentation.....	12
	4. Analysis	12
	5. Criterion for Successful Policy	13
	6. Output	13
	7. Organization of Chapters.....	13
II.	CURRENT STATE—THE SECURITY CLEARANCE BACKLOG.....	15
A.	OBTAINING SECURITY CLEARANCES.....	15
B.	NATIONAL BACKGROUND INVESTIGATIONS BUREAU.....	17
C.	SECURITY CLEARANCE BACKLOG IMPACTS.....	20
D.	INFORMATION CLASSIFICATION TRENDS	23
III.	POLICY OPTIONS REVIEWED.....	27
A.	POLICY OPTION CRITERIA	27
B.	POLICY OPTION 1: CURRENT PROCESS WITH THE ADDITION OF THE CONTINUOUS EVALUATION DEVELOPMENTAL APPROACH	27
	1. Policy Option 1 Benefits	28
	2. Policy Option 1 Challenges	30
	3. Policy Option 1 Outcome Assumptions.....	33

C.	POLICY OPTION 2: INCREASE THE NUMBER OF NATIONAL BACKGROUND INVESTIGATIONS BUREAU INVESTIGATORS TRANSITIONAL APPROACH.....	34
1.	Policy Option 2 Benefits	37
2.	Policy Option 2 Challenges	37
3.	Policy Option 2 Outcome Assumptions.....	38
D.	POLICY OPTION 3: LIMIT CLEARANCE POPULATION TO INVESTIGATOR THROUGHPUT TRANSFORMATIONAL APPROACH.....	38
1.	Policy Option 3 Benefits	41
2.	Policy Option 3 Challenges	42
3.	Policy Option 3 Outcome Assumptions.....	42
IV.	FINDINGS.....	45
A.	DEVELOPMENTAL APPROACH—ADDING ANNUAL CONTINUOUS EVALUATION TO THE CURRENT SECURITY CLEARANCE PROCESS	45
B.	TRANSITIONAL APPROACH—HIRING ADDITIONAL BACKGROUND INVESTIGATORS.....	45
C.	TRANSFORMATIONAL APPROACH—LIMITING ANNUAL INVESTIGATIONS TO NBIB THROUGHPUT	46
V.	CONCLUSION	49
A.	BEST POLICY.....	49
B.	LIMITING FACTORS.....	49
C.	IMPLEMENTATION CHALLENGES	49
D.	SUGGESTIONS FOR FUTURE RESEARCH.....	50
	LIST OF REFERENCES.....	53
	INITIAL DISTRIBUTION LIST	57

LIST OF FIGURES

Figure 1.	National Background Investigations Bureau Rates by Investigation FY 2018 Type	18
Figure 2.	National Background Investigations Bureau Projected Billing Rates FY 2019	19
Figure 3.	National Background Investigations Bureau Projected Billing Rates FY 2020	20
Figure 4.	Security Clearance Population 2013–2019.....	22
Figure 5.	Original Classification Activity FY 2008–FY 2017.....	25
Figure 6.	Total Number of Pages Reviewed and Declassified FY 2008–FY 2017.....	26
Figure 7.	Average Timeliness for Processing the Fastest 90 Percent of Security Clearance Cases	31
Figure 8.	National Background Investigations Bureau Investigation Fieldwork Intensiveness FY 2005–FY 2018.....	32
Figure 9.	Eligible, in Access Population CY 2017.....	39
Figure 10.	Eligible, Not in Access CY 2017	39
Figure 11.	Security Clearance Investigation Backlog by Investigation Type.....	40
Figure 12.	Causes of Security Clearance Investigation Delays.....	51

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	ODNI Annual Report on Security Clearance Determinations Agency Security Clearance Denials and Revocations FY 2017	29
Table 2.	Policy Option Comparison Model	46

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACES	Automated Continuous Evaluation System
ASGVA	Australian Government Security Vetting Agency
CEO	chief executive officer
DOD	Department of Defense
GAO	Government Accountability Office
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
NBIB	National Background Investigations Bureau
PAC	Performance Accountability Council

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

To protect sensitive information, certain positions in the federal government require candidates to obtain and maintain a security clearance. Security clearances help ensure that an individual is trustworthy and capable of handling sensitive information, which has the potential of harming the United States if divulged.¹ From 2014 to 2018, the backlog of investigations increased from approximately 190,000 to 710,000.² A candidate can expect to wait for a fully adjudicated Secret clearance between 153–197 days while the wait for a Top Secret clearance is between 134 to 395 days.³ This wait time is considered the current norm; however, the guidelines in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) set performance measures of 60 days to complete investigations and adjudicate security clearances.⁴

Literature in the fields of information security, personnel security, risk management, and organizational change form the basis for the theoretical concepts that may improve the security clearance process in the United States. Legal authorities, expert testimony, and government reports relating to the security clearance process in the United States serve as a guide to determine what measures are legally required for government departments and agencies to ensure the integrity of sensitive information, as well as establish metrics for government performance. The security clearance process in the United States was analyzed with these factors in mind to determine whether changes in policies

¹ Michelle Christenson, *Security Clearance Process: Answers to Frequently Asked Questions*, CRS Report No. R43216 (Washington, DC: Congressional Research Service, 2016), 1, <https://fas.org/sgp/crs/secrecy/R43216.pdf>.

² Government Accountability Office, *Testimony before the Select Committee on Intelligence, U.S. Senate, Personnel Security Clearances, Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations Statement of Brenda S. Farrell, Director, Defense Capabilities and Management*, GAO-18-431T (Washington, DC: Government Accountability Agency, 2018), 1, <https://www.intelligence.senate.gov/sites/default/files/documents/os-bfarrell-030718.pdf>.

³ National Counterintelligence and Security Center, *2015 Annual Report on Security Clearance Determinations* (Washington, DC: Office of the Director of National Intelligence, 2016), 8, <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2016/item/1603-2015-annual-report-on-security-clearance-determinations>.

⁴ Office of the Director of National Intelligence, *IRTPA Title III Annual Report for 2010* (Washington, DC: Office of the Director of National Intelligence, 2011), 1, <https://fas.org/irp/dni/irtpa-2011.pdf>.

and procedures might improve the timeliness of security clearance background investigations and adjudications while recruiting and maintaining trustworthy personnel.

A policy options analysis was conducted to evaluate potential improvements to the security clearance process. Policy recommendations focused on the incorporation of two specific Government Accountability Office recommendations, the investigation backlog and investigator capacity, in addition to novel criteria that considers foundational concepts in information security, risk management, and organizational change. Policy options included maintaining the current system while adding annual continuous evaluation, hiring additional National Background Investigations Bureau (NBIB) investigators to reduce the security clearance backlog, and limiting the clearance population to NBIB investigator throughput.

A cost-benefit analysis was developed for each policy option that depicted the notional process along with associated risks and opportunities, and assumptions for the implementation of each policy. The proposed policies were evaluated for improvements to the security clearance investigation quality, increased timeliness to the security clearance investigation process, and potential cost increases or decreases to security clearance investigations. An alternate solution matrix was created to synthesize the positives and negatives of each policy recommendation.

Policy options employed either a developmental, transitional, or transformational approach to organizational change. Developmental change is notionally the least amount of difficult change, while transitional change is notionally a moderate organizational change and transformational change is notionally the most difficult organizational change.⁵ Presently, the NBIB is responsible for approximately 90 percent of the security clearance background investigation workload.⁶ Policies suggested are for the use and consideration

⁵ Ann L. Cunliffe and John T. Luhman, “Organizational Change,” in *SAGE Key Concepts Series: Key Concepts in Organization Theory—Credo Reference*, ed. Ann L. Cunliffe and John T. Luhman (London: Sage, 2013), 1, https://search.credoreference.com/content/entry/sageukot/organizational_change/0.

⁶ United States Office of Personnel Management, *Statement of Charles S. Phalen, Jr., Director, National Background Investigations Bureau, U.S. Office of Personnel Management before the Select Committee on Intelligence United States Senate on “Security Clearance Reform”* (Washington, DC: United States Office of Personnel Management, 2018), 1, <https://www.intelligence.senate.gov/sites/default/files/documents/os-cphalen-030718.pdf>.

of the NBIB. It should be noted that with the looming reorganization of the NBIB, and the transferring of background investigation roles and responsibilities back to the Department of Defense for their staff, these policy suggestions and approaches would only be altered slightly, but still recommended regardless of the reorganization status due to the large challenge that the security clearance backlog poses.⁷ For the purposes of the following recommendations, the author assumed that the NBIB would still maintain its current role and share of the investigation burden.

A. DEVELOPMENTAL APPROACH—ADDING ANNUAL CONTINUOUS EVALUATION TO THE CURRENT SECURITY CLEARANCE PROCESS

The developmental approach to changing how the NBIB currently conducts background investigations consists of adding a requirement to run national agency checks on holders of security clearances annually. This approach expands on how the NBIB currently conducts investigations by validating that users who have access to sensitive information are trustworthy by increasing the frequency of individual reinvestigation to allow more frequent checks for indicators of maladaptive behaviors. By increasing the frequency of reinvestigation across the security clearance population, information security has a higher likelihood of being protected from insider threat due to this increase in the quality of the investigation. This approach, however, would not reduce the security clearance backlog, nor would it reduce costs associated with background investigations since more time and money would be required to process more frequent reinvestigations across the security clearance population.

B. TRANSITIONAL APPROACH—HIRING ADDITIONAL BACKGROUND INVESTIGATORS

The transitional approach to organizational change within the NBIB focuses on increasing investigator capacity by hiring additional investigators. This approach would bring the NBIB into an environment where they would be able to meet the current demands

⁷ Nicole Ogrysko, “DoD to Reorganize, Create New Security Clearance Organization,” Federal News Network, November 20, 2018, <https://federalnewsnetwork.com/reorganization/2018/11/dod-to-reorganize-create-new-security-clearance-organization/>.

for security clearance investigations, make improvements in information security, investigation quality, and reduce the security clearance backlog. With investigators having more time to focus on a lesser workload, the quality of investigations would increase. Since more time could be spent per investigation, theoretically, the individuals being granted security clearances would have a higher likelihood that their investigations were not rushed, and therefore, would be trustworthy with sensitive information and thus make positive gains in increasing information security. This approach would also result in an increase in cost to the security clearance process, since the NBIB would have to increase its staff from 7,200 to approximately 29,000 to reduce the security clearance backlog.

C. TRANSFORMATIONAL APPROACH—LIMITING ANNUAL INVESTIGATIONS TO NBIB THROUGHPUT

Limiting the annual security clearance investigations to the throughput that the NBIB could still manage to conduct quality investigations would transform the operating environment for the NBIB, as well as for departments and agencies that rely on the NBIB for investigation support.

Since the ideal caseload for the current staff of NBIB investigators is between 160,000–180,000⁸ investigation products per year to include novel investigations and reinvestigations, this suggested policy will limit the amount of novel clearances and reinvestigations completed on an annual basis until the security clearance backlog is cleared.

This approach would reduce the backlog of security clearances over time, improve information security, and increase the quality of background investigations by allowing more time per investigation product for the current NBIB investigator staff. This approach would not result in cost increases to the security clearance process since no new staff or technology would be required to implement it.

⁸ United States Office of Personnel Management, *Statement of Charles S. Phalen, Jr.*, 2.

D. RESULTS

The following table shows that the transformational approach may notionally result in the most improvements. Limiting the number of investigations and reinvestigations to NBIB investigation throughput can possibly reduce the security clearance investigation backlog, increase the quality of investigations, as well as increase information security.

	Does policy reduce security clearance investigation backlog? If so, add 1 point.	Does policy improve information security? If so, add 1 point.	Does policy increase potential costs to security clearance process? If so, subtract 1 point.	Does policy increase quality of investigation? If so, add 1 point.	Total
Adding Annual Continuous Evaluation to the Current Security Clearance Process	+/-0	+1	+/-0	+1	2
Hire Additional Background Investigators	+1	+/-0	-1	+1	2
Reduce Clearance Population to Investigator Throughput	+1	+1	+/-0	+1	3

E. CONCLUSION

Based on the analysis, limiting the clearance population to the background investigator throughput achieves the best total positive outcome in the security clearance process. This policy option decreases the backlog by reducing the demand of investigations on security clearance investigators. Positive outcomes are gained in the quality of investigation by allowing investigators to take more time on their investigation products since they will have a sharply decreased caseload. This policy option also has the potential to improve information security by decreasing the number of individuals with access to classified information; the fewer individuals with access, the lower the chances are for system breaches by insider threat.

The challenge to this transformational approach in addressing this problem is that the potential capacity of work in the homeland defense and national security space becomes

limited. Cutting the number of individuals supporting homeland security and national defense missions without a phased approach could result in inadequate staffing to complete related missions. The limitation to fixing the number of cleared population to investigator capacity is that a significant amount of time would be required to develop staffing and workload transition plans to adapt to this new environment.

A potential also exists for a limited capability of staff to share sensitive and classified information between the interagency. While reducing the population with security clearances helps reduce the amount of threats that can impact sensitive information, it may limit the ability of the U.S. government to complete its national defense and homeland security mission.

I. THE SECURITY CLEARANCE BACKLOG—A HOMELAND SECURITY CHALLENGE

A. BACKGROUND

From 2014–2018, the U.S. federal government security clearance backlog increased from 190,000 investigations to 710,000 investigations.¹ The backlog of security clearance investigations has resulted in investigation timelines that range between 134 and 395 days.² While candidates wait for their security clearances, critical work in homeland and national security goes unstaffed. In addition, the security clearance backlog has compounding issues that impact attracting new talent to the homeland and national security mission, as well as driving up competition for cleared candidates that leads to higher prices for cleared candidates.

While risk tolerance varies by agency, the consequences for performing low quality investigations are evident in recent security breaches, such as leaks of classified information from Chelsea Manning and Edward Snowden, as well as the mass shootings in Fort Hood, Texas, by Nidal Hasan, and the Navy Yard shooting perpetrated by Aaron Alexis.³ In all these cases, the individuals held security clearances. Despite these events being relatively low frequency, their impact to the United States was high in both information integrity and in lost lives.

The organization that handles over 90 percent of the caseload for background investigations, the National Background Investigations Bureau (NBIB), has the capability to provide approximately 160,000–180,000 investigations annually. With the current

¹ Government Accountability Office, *Testimony before the Select Committee on Intelligence, U.S. Senate, Personnel Security Clearances, Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations Statement of Brenda S. Farrell, Director, Defense Capabilities and Management*, GAO-18-431T (Washington, DC: Government Accountability Agency, 2018), 1, <https://www.intelligence.senate.gov/sites/default/files/documents/os-bfarrell-030718.pdf>.

² National Counterintelligence and Security Center, *2015 Annual Report on Security Clearance Determinations* (Washington, DC: Office of the Director of National Intelligence, 2016), 8, <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2016/item/1603-2015-annual-report-on-security-clearance-determinations>.

³ Department of Defense, *Internal Review of the Washington Navy Yard Shooting* (Washington, DC: Department of Defense, 2013), 45.

staffing structure, the NBIB can handle approximately 25 percent of the caseload.⁴ Changes in policy can be considered to address this critical issue; however, drastic change may be required to address this issue. At the time this thesis is being completed, the Trusted Workforce 2.0 framework is scheduled to be released in the coming weeks.⁵ The Trusted Workforce 2.0 initiative hopes to make improvements to the overall security clearance background investigation process by allowing background investigators to employ digital options for interviews and increase the frequency of clearance holder reinvestigations.⁶ These changes are likely to be welcome, but they will do little to reduce the large backlog that has developed in recent years, and it is likely that the recommendations in this thesis will be more important than ever.

This thesis recommends a transformational organizational change to the NBIB be recommended to address the backlog of security clearance investigations. A policy change that limits the annual amount of security clearance investigations to the throughput of the NBIB may reduce the backlog of security clearance investigations, as well as increase the quality of investigations and the integrity of national security information without adding to the costs of security clearances.

B. PROBLEM STATEMENT

To protect sensitive information, certain positions in the federal government require candidates to obtain and maintain a security clearance. Security clearances help ensure that an individual is trustworthy and capable of handling sensitive information, which has the potential of harming the United States if divulged.⁷ From 2014 to 2018, the backlog of

⁴ United States Office of Personnel Management, *Statement of Charles S. Phalen, Jr., Director, National Background Investigations Bureau, U.S. Office of Personnel Management before the Select Committee on Intelligence United States Senate on "Security Clearance Reform"* (Washington, DC: United States Office of Personnel Management, 2018), 2, <https://www.intelligence.senate.gov/sites/default/files/documents/os-cphalen-030718.pdf>.

⁵ "The Security Clearance Process Is About to Get Its Biggest Overhaul in 50 Years," Nextgov, 1, accessed March 9, 2019, <https://www.nextgov.com/cio-briefing/2019/02/security-clearance-process-about-get-its-biggest-overhaul-50-years/155229/>.

⁶ Nextgov, 1.

⁷ Michelle Christenson, *Security Clearance Process: Answers to Frequently Asked Questions*, CRS Report No. R43216 (Washington, DC: Congressional Research Service, 2016), 1, <https://fas.org/sgp/crs/secrecy/R43216.pdf>.

investigations increased from approximately 190,000 to 710,000.⁸ A candidate can expect to wait for a fully adjudicated Secret clearance between 153–197 days while the wait for a Top Secret clearance is between 134 to 395 days.⁹ This wait time is considered the current norm; however, the guidelines in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) set performance measures of 60 days to complete investigations and adjudicate security clearances.¹⁰

The delay in security clearance processing has negative consequences for the homeland security enterprise. Kevin Phillips, CEO of ManTech Inc., and a major support contractor to the U.S. government, testified before the Senate Select Committee on Intelligence regarding the impact on the homeland security mission. According to Phillips:

The current backlog of over 700,000 clearance cases constitutes a major national security issue—it is not a “back-office” administrative function. The slow pace of the security clearance process prevents us from recruiting and hiring the talented individuals critical to national security. Specific areas impacted include weapon systems, space missions and operations, cyber network operations and cyber security, cloud computing, data science and analytics, and hardware manufacturing. Nationwide, technology professionals are in high demand. They will not wait for a year or longer to obtain a clearance to begin the meaningful work which contributes to the innovations demanded by national security priorities.¹¹

Phillips goes on to project that approximately 10,000 critical national security contract positions remain unfilled because of the current security clearance backlog.¹²

On March 7, 2018, David Berteau, president and CEO of the Professional Services Council, also testified before the Senate Select Committee on Intelligence. Berteau voiced

⁸ Government Accountability Agency, *Testimony before the Select Committee on Intelligence, U.S. Senate, Personnel Security Clearances, Additional Actions Needed*, 1.

⁹ National Counterintelligence and Security Center, *2015 Annual Report on Security Clearance Determinations*, 8.

¹⁰ Office of the Director of National Intelligence, *IRTPA Title III Annual Report for 2010* (Washington, DC: Office of the Director of National Intelligence, 2011), 1, <https://fas.org/irp/dni/irtpa-2011.pdf>.

¹¹ Senate Select Committee on Intelligence, *Statement of Kevin Phillips, CEO ManTech Inc., Hearing on Security Reform* (Washington, DC: Senate Select Committee on Intelligence, 2018), 2, <https://www.intelligence.senate.gov/sites/default/files/documents/os-kphillips-030718.pdf>.

¹² Senate Select Committee on Intelligence, 2.

his concern about items that contribute to the backlog. Using an example of verifying an applicant's academic history Berteau stated:

Currently, to verify an applicant's educational background, an investigator must draft, print and hard mail a letter to the college or university cited. The investigator then waits for the college or university to respond—again via hard mail—with a verification of the applicant's information. Once the verification letter is received, the investigator scans it into their system and adds it to the applicant's file. This example highlights the outdated, cumbersome, and lengthy process now used to simply confirm that an applicant attended the college they claim to have attended.¹³

C. RESEARCH QUESTION

How can the U.S. government reduce the security clearance backlog and process security clearance investigations and adjudications efficiently while maintaining the quality of personnel and security of sensitive information?

D. LITERATURE REVIEW

This literature review provides an overview of the academic fields that conceptually contribute to successful security. This literature review also includes government reports and expert testimony that have underscored the threat to national security posed by the backlog of security investigations and adjudications. The fields of information security, personnel security, risk management, organizational change the laws governing security clearances, as well as government reports and expert testimony on security clearances are analyzed to develop potential solutions and policy options for implementation to improve the security clearance process.

1. Information Security

According to Janczewski and Colarik, information security is a critical component of safeguarding information that becomes classified and accessed by authorized individuals. Having secure information systems guarantees that accurate, inalterable

¹³ Senate Select Committee on Intelligence, *Statement of David J. Berteau, President & CEO, Professional Services Council, before the Senate Select Committee on Intelligence* (Washington, DC: Senate Select Committee on Intelligence, 2018), 6, <https://www.intelligence.senate.gov/sites/default/files/documents/os-dberteau-030718.pdf>.

information is available by system users.¹⁴ In the context of security clearances, information security would be best related to the systems that protect classified information. Expanding on this concept, White describes principles on which organizations can focus to ensure information systems achieve confidentiality, integrity, availability, and assurance.¹⁵ The principle of confidentiality refers to the correct user or device having access to and control of the information within a system. Information integrity is the concept that the data being accessed have not been changed or corrupted and remain intact throughout a data transaction process. Availability of information references the capability of users to access data when required. Finally, information system assurance is the validation that confidentiality, integrity, and availability are successfully achieved.¹⁶ Scholars prioritize each of the components of information security previously described differently, but consensus exists that the successful application of these concepts enables secure information systems. While literature that focuses on information security and its relationship to security clearances is sparse, information security literature can help highlight certain components within information classification and the security clearance process that may be considered to improve information security of national security information.

2. Personnel Security

Personnel security programs work to ensure that individuals are trustworthy to carry out the roles and responsibilities of their positions. Positions in the federal government are categorized based on their sensitivity. Individuals with more sensitive positions undergo more stringent background investigations.¹⁷ Janczewski and Colarik suggest that organizations can take measures to mitigate the threats posed by malevolent employees by

¹⁴ Lech J. Janczewski and Andrew M. Colarik, *Managerial Guide for Handling Cyber-Terrorism and Information Warfare* (Hershey, PA, Idea Group Publishing, 2005), 1–23, <https://doi.org/10.4018/978-1-59140-583-2.ch001>.

¹⁵ Jay D. White, *Managing Information in the Public Sector* (Armonk, NY: M.E. Sharpe, Inc., 2007), 218–237, <https://ebookcentral.proquest.com/lib/ebook-nps/detail.action?docID=302467>.

¹⁶ White, 218.

¹⁷ Office of Inspector General, *The DHS Personnel Security Process*, OIG Report No. OIG-09-65 (Washington, DC: Department of Homeland Security, 2009), 2, <https://permanent.access.gpo.gov/gpo/14559/OIG09-65May09.pdf>.

implementing employee pre-screening that requires prospective employees sign a non-disclosure agreement, and create employee training on the proper use of technological systems to maintain a secure system environment.¹⁸ While these measures may stop the majority of bad actors, in the context of security clearances and classified information, these types of measures failed to protect the U.S. government from security breaches of classified information like those of Chelsea Manning and Edward Snowden.¹⁹

Breaches to a secure system can still frequently emerge from individuals screened and deemed trustworthy. A subset of literature within personnel security addresses the insider threat phenomenon. Claycomb et al. describe the insider threat as “a malicious . . . current or former employee, contractor, or other business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.”²⁰ Factors that influence the frequency of insider threats emerging have been researched. According to Kramer, individuals have more access to diverse ideas through easier international travel and indirect exposure and contact to potential corrupting influences through easy access to the internet while simultaneously having access to large amounts of classified information.²¹ Existing literature on the insider threat and personnel security highlight factors critical in the security clearance process in regards to selecting trustworthy individuals who will safeguard sensitive information.

¹⁸ Janczewski and Colarik, *Managerial Guide for Handling Cyber-Terrorism and Information Warfare*, 163–174.

¹⁹ Graham Lanktree, “Leaker Chelsea Manning Reveals for the First Time Why She Released Secret Military and Diplomatic Documents,” *Newsweek*, June 9, 2017, <https://www.newsweek.com/chelsea-manning-interview-reveals-why-she-leaked-secret-military-documents-623668>.

²⁰ William R. Claycomb et al., “Chronological Examination of Insider Threat Sabotage: Preliminary Observations,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 3, no. 4 (December 2012): 4, <http://isyou.info/jowua/papers/jowua-v3n4-1.pdf>.

²¹ Lisa A. Kramer, *Technological, Social and Economic Trends that Are Increasing U.S. Vulnerability to Insider Espionage*, Technical Report Number 05-10 (Monterey, CA: Defense Personnel Security Research Center, 2005), ix, <https://fas.org/sgp/othergov/dod/insider.pdf>.

3. Risk Management

Organizations employ risk management principles to ensure that their objectives can still be met despite disruptions. Hubbard posits that to pursue opportunities and gains, organizations may expose themselves to risks that have the potential to damage them; however, they can mitigate the potential for damage to the best of their abilities depending on the resources they have available. An agreed upon approach to risk management (i.e., obtaining insurance to transfer the risk for flood to a physical structure) can identify risks and develop cost effective measures to offset the potential for loss.²² Government organizations lessen potential risks from new employees by assessing the character and trustworthiness and determining the potential damage that can be done in their prospective position in the pre-employment screening phase.

Risk management programs involve a holistic approach that addresses risk factors at the organizational, business process, and the operating environment levels.²³ The literature on risk management describes how organizations can logically approach risk mitigation from a variety of threats and from different facets of their operational organization. Government organizations are required by law to take measures to avoid organizational risk; employee screening and vetting is one way agencies accomplish this task.²⁴ The next section outlines the concepts in organizational change that can be used to determine how easily an organization can shift operations based on its environment.

²² Douglas W. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It* (Hoboken, NJ: Wiley, 2009), 26–28.

²³ Department of Commerce, *Guide for Applying the Risk Management Framework to Federal Information Systems a Security Life Cycle Approach*, rev. 1 (Gaithersburg, MD: Department of Commerce, 2010), 1, <https://permanent.access.gpo.gov/lps121083/sp800-37-rev1-final.pdf>.

²⁴ Barack Obama, Executive Order 13526 of December 29, 2009, “Classified National Security Information,” *Code of Federal Regulations*, title 3 (2010): 720, <https://www.gpo.gov/fdsys/pkg/FR-2010-01-05/pdf/E9-31418.pdf>.

4. Organizational Change

Organizational change is the study of how organizations transform from their current state to their ideal state.²⁵ What yields the most positive outcome in organizational change is debated among scholars. According to Cunliffe and Luhman, organizational change can be either developmental, transitional or transformational. Developmental organizational changes are those that make improvements to current processes and structures. Transitional organizational change moves an organization to a known operating

n (directed change, planned change, and guided changing), a strong bias exists in allowing for organizational participation through the change process. Kerber and Buono argue that the situation and the environment may dictate the type of change an organization implements. Direct environment. Transformational change forces organizations to move to an operating environment with several variables with which organization members may be unfamiliar.²⁶

Kurt Lewin, an expert on organizational change, suggests a model that describes change as a process of unfreezing, movement, and refreezing. Organizations identify a need for change, execute changes, and then solidify the changes within their organization.²⁷ David Cooperrider, an organizational change scholar, by contrast, believes that appreciative inquiry is the best way to move an organization through change. Appreciative inquiry involves polling the individuals within an organization to build narratives for how they want the organization to operate and achieve its ideal mission, develop a participatory environment, and then use a plan to implement those changes.²⁸

Kenneth Kerber and Anthony Buono maintain that in the three common types of change implemented within an organization change may disenfranchise organization members if leaders within the organization who force the change do not adequately provide

²⁵ Ann L. Cunliffe and John T. Luhman, "Organizational Change," in *SAGE Key Concepts Series: Key Concepts in Organization Theory—Credo Reference*, ed. Ann L. Cunliffe and John T. Luhman (London: Sage, 2013), 1, https://search.credoreference.com/content/entry/sageukot/organizational_change/0.

²⁶ Cunliffe and Luhman, 1.

²⁷ Cunliffe and Luhman, 1.

²⁸ Cunliffe and Luhman, 1.

tools for coping with the emotional impact of the change. Planned change provides a guide for organizational members to understand novel change that can reduce obstruction to new requirements, but often times may be too confusing for organization members if executed incorrectly. Guided changing relies on an iterative learning and adapting approach to organizational change. Organization members incorporate feedback with the end state of continually improving processes; however, continual change may leave organization members in a state of prolonged disorientation.²⁹ Selecting a method of organizational change can be the most successful if the environmental conditions are carefully analyzed prior to the change taking place.

Several approaches to organizational change exist that can be applied to the security clearance backlog. The theoretical foundations for developmental, transitional, and transformational change are considered in the development of policy options to reduce the backlog of security clearance investigations. Additionally, policy options are developed with common barriers to successful organizational change in mind.

5. Authorities

Government organizations have legal requirements to fulfill when hiring individuals for positions that require security clearances. The chief law governing security clearances is 50 U.S.C. § 3341. This law outlines agency responsibilities for hiring employees with security clearances, sets performance criteria for security clearance investigations and process length, as well as sets timelines for reporting progress.³⁰ The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) establishes requirements for agencies to complete the fastest 90 percent of background investigations within 60 days.³¹ Executive Order 13526, Classified National Security Information, prescribes a “uniform system for classifying, safeguarding, and declassifying national

²⁹ Kenneth Kerber and Anthony F. Buono, “Rethinking Organizational Change: Reframing the Challenge of Change Management,” *Organization Development Journal; Chesterland* 23, no. 3 (Fall 2005): 23–38.

³⁰ National Security Act of 1947, Public Law 108–458, 50 U.S.C. § 3341 (2004) <https://www.law.cornell.edu/uscode/text/50/3341>.

³¹ S. 2845, 115th Cong., 2nd sess. (2017–2018), https://fas.org/irp/congress/2004_rpt/s2845-summ.pdf.

security information, including information relating to defense against transnational terrorism.”³² This executive order also describes the criteria for security clearances by level and the associated damages resulting in unintentional disclosure of sensitive information at each classification level.³³ The rules and laws governing the classification of sensitive information and vetting of individuals who require a security clearance are well established.

6. Government Reports and Current Recommendations

The Government Accountability Office (GAO) analyzed the main areas in which the U.S. government was experiencing challenges regarding the security clearance process. The main issues recognized by the GAO were investigation backlog, investigator capacity, clearance processing delays, a lack of quality measures for investigations, security clearance reform delays, and IT security.³⁴ The GAO recommended that the Office of the Director of National Intelligence, Office of Management and Budget/National Background Investigation Bureau, and the Department of Defense (DOD) work together to reduce the investigation backlog, increase total investigator capacity, and improve the quality of background investigations.³⁵ The GAO has made recommendations that could improve conditions resulting in a reduction to the security clearance backlog. In addition to the GAO, industry experts have provided testimony on the extent of the security clearance backlog and its impacts to homeland security and national defense.

Chief executive officers (CEOs) of major government contracting firms like Kevin Phillips of Man Tech Inc. have provided testimonies before Congress to describe the impact of the security clearance backlog to national security. By Phillips’ calculations, approximately 10,000 positions in critical national security sectors went unfilled due to the

³² Obama, Executive Order 13526, 707.

³³ Obama, 707–708.

³⁴ Government Accountability Office, *High Risk: Government-Wide Personnel Security Clearance Process*, GAO-17-317 (Washington, DC: Government Accountability Office, 2017), 1, https://www.gao.gov/highrisk/govwide_security_clearance_process/why_did_study.

³⁵ Government Accountability Office, 1.

security clearance backlog.³⁶ The security clearance backlog can theoretically result in entire sectors of work being incomplete due to the lack of cleared staff available.

The causes of the current state of the security clearance backlog are attributed to different events and issues according to different experts. Charles Phalen, director of the National Background Investigations Bureau, attributes part of the current security clearance backlog to events like the loss of a major government support contractor in 2014. This loss resulted in 64 percent of the investigative capacity for security clearances being removed.³⁷ This capacity loss brought investigations at that time to a standstill as the government struggled to rebuild that capacity. While events like the loss of a major support contractor definitely had a role to play in the current state of the security clearance backlog, some government officials believe that the core of the issue lies in the way investigations are being conducted. David Berteau, president and CEO of the Professional Services Council, has stated that the nature of background investigations for security clearances does not adequately take advantage of technology to expedite simple pieces in the investigative process. For Berteau, capitalizing on opportunities to improve areas where investigators are still required to make inquiries using written forms for verification may add up to great reductions in the overall investigation timeline.³⁸ Despite a consensus on what the main causes are and contributing factors to the security clearance backlog, it is well documented through expert testimony and official government reports that challenges exist within the U.S. government in regards to security clearances.

7. Summary

Literature in the fields of information security, personnel security, risk management, and organizational change form the basis for the theoretical concepts that may improve the security clearance process in the United States. Legal authorities, expert testimony, and government reports relating to the security clearance process in the United States serve as a guide to determine what measures are legally required for government

³⁶ Senate Select Committee on Intelligence, *Statement of Kevin Phillips*, 2.

³⁷ United States Office of Personnel Management, *Statement of Charles S. Phalen, Jr.*, 2.

³⁸ Senate Select Committee on Intelligence, *Statement of David J. Berteau*, 5–6.

departments and agencies to ensure the integrity of sensitive information, as well as establish metrics for government performance. The security clearance process in the United States are analyzed with these factors in mind to determine whether changes in policies and procedures might improve the timeliness of security clearance background investigations and adjudications while recruiting and maintaining trustworthy personnel.

E. RESEARCH DESIGN

1. Object of Study

The object of study for this thesis is the current background investigation and adjudication process for security clearances in the United States. The security clearance process in the United States is analyzed to identify potential areas for process improvement. Alternative processes and approaches are also reviewed to improve outcomes in balancing information security and investigation timeliness.

2. Limitations and Scope

This thesis examines the security clearance process in the United States as it pertains to federal employees and contractors. While it evaluates different types of security clearances and background investigation requirements of each clearance, this thesis does not focus on the access types within each category (e.g., Top Secret clearances with Sensitive Compartmented Information) nor does it focus on suitability determinations.

3. Instrumentation

Open-source data from government organizations and congressional testimony on the security clearance backlog are used to evaluate the current government performance of security clearance investigations. After-action reports from data breaches and personnel security failures are also included to provide a baseline perspective to the problem set.

4. Analysis

A policy options analysis is conducted to evaluate potential improvements to the security clearance process. Draft policy options focus on the incorporation of two specific GAO recommendations (the investigation backlog and investigator capacity) in addition to

novel criteria that consider foundational concepts in information security, risk management, and organizational change.

Policy options include:

- Maintain the current system with the additional of continuous evaluation
- Hire additional investigators to reduce the backlog
- Limit clearance population to investigation throughput

5. Criterion for Successful Policy

A cost-benefit analysis is developed for each policy option to depict the notional process along with associated risks and opportunities, and assumptions for the implementation of each policy. The proposed policies are evaluated for improvements to the security clearance investigation quality, increased timeliness to the security clearance investigation process, and potential cost increases or decreases to security clearance investigations. An alternate solution matrix is created to synthesize the positives and negatives of each policy recommendation. Finally, recommendations are selected and defended based on an analysis of policy efficacy.

6. Output

The output of this thesis research and analysis are recommendations to improve efficiencies of the security clearance investigation process while maintaining the quality of personnel and security of sensitive information.

7. Organization of Chapters

Chapter II describes the purposes of security clearances and the background of the issues that have led to the backlog of security clearance investigations, and adjudicates current trends in information classification and potential issues that may result from a prolonged backlog of security clearance investigations. Chapter III describes three different policy options that may improve the security clearance investigation backlog without sacrificing the security of national security information. Chapter IV provides a comparative

analysis between the three proposed policy options. Lastly, Chapter V summarizes conclusions of the research and analysis and provides an explanation of the recommended policy.

II. CURRENT STATE—THE SECURITY CLEARANCE BACKLOG

A. OBTAINING SECURITY CLEARANCES

Certain positions in the federal government require federal employees or contractors to maintain a security clearance. Security clearances are used to ensure that individuals can be trusted with sensitive national security information. A security clearance is a determination that individuals are eligible to access classified information.³⁹

The clearance levels (least to most sensitive) are Confidential, Secret, and Top Secret.⁴⁰ Each category of clearance has an associated level of potential damage associated with it. Disclosure of Top Secret information is “expected to cause exceptionally grave damage to the national security,” Secret information disclosure is “expected to cause serious damage to national security,” while Confidential information is “expected to cause damage to national security.”⁴¹

Individuals who wish to obtain national security positions in the federal government that requires access to classified material must complete a process to become part of the workforce. For positions that require security clearances, the main components of this process are pre-investigation, investigation, adjudication, and reinvestigation.⁴² Regardless of which agency the candidates are applying to, this process of investigation and adjudication is the same.

During the pre-investigation phase, the hiring agency determines "that an employee or contractor requires access to classified information for the completion of his or her duties".⁴³ The prospective employees then submit their clearance applications, which is

³⁹ Christenson, *Security Clearance Process*, 1.

⁴⁰ Christenson, 2.

⁴¹ Obama, Executive Order 13526, 707–708.

⁴² Christenson, *Security Clearance Process*, 6.

⁴³ Christenson, 6.

commonly known as Standard Form 86, Questionnaire for National Security Positions.⁴⁴ This form is the same across agencies and asks the same security questions of all applicants.

The investigation phase verifies the information provided by the candidates in the application through a background investigation. Usually, the sensitivity level determines the length of personal history examined. Investigative instruments, such as personal interviews and polygraphs, can be used depending upon the sensitive nature of the position.⁴⁵ Candidates for security clearances may be interviewed in person or virtually.

Information that the candidates provides in their questionnaire to the background investigator is submitted to the agency adjudicator, which is the final step of the process for obtaining a security clearance. The information vetted during the background investigation phase is provided to the agency that requested the investigation be performed. The agency makes the final determination of whether the candidates receive a security clearance.⁴⁶

Once the candidates are hired and have active security clearances, a maintenance protocol exists to ensure the employees can still be trusted to access classified material to perform their official duties. This reinvestigation phase varies depending on the type of clearance held by the individuals. For a Confidential clearance, reinvestigations occur every 15 years. For a Secret clearance, the reinvestigation occurs at least every 10 years. Top Secret clearance reinvestigations occur every five years.⁴⁷

The criteria that agencies use to determine whether candidates receive security clearances are uniform. Michelle Christenson of the Congressional Research Service outlines the 13 adjudicative guidelines whereby security clearance candidates are reviewed:

- (1) Allegiance to the United States;
- (2) Foreign Influence;
- (3) Foreign Preference;
- (4) Sexual Behavior;
- (5) Personal Conduct;
- (6) Financial Considerations;
- (7) Alcohol Consumption;
- (8) Drug Involvement;
- (9)

⁴⁴ Christenson, 6.

⁴⁵ Christenson, 6.

⁴⁶ Christenson, 6.

⁴⁷ Christenson, 6.

Psychological Conditions; (10); Criminal Conduct; (11) Handling Protected Information; (12) Outside Activities; and (13) Use of Information Technology Systems.⁴⁸

These criteria help to ensure that adjudicators of security clearances can make the most objective determination possible when granting candidates security clearances.

B. NATIONAL BACKGROUND INVESTIGATIONS BUREAU

The majority of personnel background investigations fall under the responsibility of the NBIB; the sponsoring agency pays the NBIB to perform this function. The NBIB is responsible for nearly 95 percent of the U.S. government background investigations and provides investigation services for nearly 100 federal agencies.⁴⁹ In 2018, it was announced that the DOD was going to re-assume responsibility of background investigations for all DOD staff. The reduction of this burden on the NBIB will most likely free up investigator capacity once the transition is complete in the coming years.⁵⁰

Figure 1 displays the current investigation rates charged by the NBIB for FY 2018. The higher the tier of investigation, the more complex the investigation is, and the more it will cost. Priority cases are more costly, most likely because they have more investigation resources put toward the cases to complete them more quickly. Reinvestigations are less costly to complete than novel investigations. Figures 2 and 3 show the projected rates for NBIB background investigation services. NBIB investigation services are projected to increase in cost by FY 2020. The projected cost increases for FY 2019 and FY 2020 are not severe for single investigation products (i.e., a National Agency Check or a Tier 5 reinvestigation). It should be noted that these products when multiplied by the number of individuals receiving their initial security clearance investigations or are under reinvestigation for their current security clearances can make a significant change in cost overall.

⁴⁸ Christenson, 9.

⁴⁹ “Billing Rates,” National Background Investigations Bureau, United States Office of Personnel Management,” accessed December 4, 2018, <https://nbib.opm.gov/hr-security-personnel/investigations-billing-rates-resources/billing-rates/>.

⁵⁰ Nicole Ogrysko, “DoD to Reorganize, Create New Security Clearance Organization,” Federal News Network, November 20, 2018, <https://federalnewsnetwork.com/reorganization/2018/11/dod-to-reorganize-create-new-security-clearance-organization/>.

Case Type		Case Type Code	Case Service	
			Standard	Priority
NAC	National Agency Check	06	\$154	<i>Not Available</i>
T1	Tier 1	63	\$194	<i>Not Available</i>
T2S	Tier 2 <i>with a Subject Interview</i>	57	\$1,550	\$1,674
T2RS	Tier 2 Reinvestigation <i>with a Subject Interview</i>	58	\$1,261	\$1,362
T3	Tier 3	64	\$433	<i>Not Available</i>
T3R	Tier 3 Reinvestigation	65	\$417	<i>Not Available</i>
T4	Tier 4	66	\$4,218	\$4,555
T4R	Tier 4 Reinvestigation	67	\$2,646	\$2,858
T5	Tier 5	70	\$5,596	\$6,043
T5R	Tier 5 Reinvestigation	71	\$3,065	\$3,310

Figure 1. National Background Investigations Bureau Rates by Investigation FY 2018 Type⁵¹

⁵¹ Source: United States Office of Personnel Management, *FY 2018 Investigations Reimbursable Billing Rates Effective October 1, 2017* (Washington, DC: National Background Investigations Bureau, 2017), 1, <https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/2017/fin-17-04.pdf>.

Case Type		Case Type Code	Case Service	
			Standard	Priority
NAC	National Agency Check	06	\$159	Not Available
T1	Tier 1	63	\$198	Not Available
T2	Tier 2	55	\$559	\$604
T2R	Tier 2 Reinvestigation	56	\$265	\$286
T2S	Tier 2 (with Subject Interview)	57	\$1,573	\$1,699
T2RS	Tier 2 Reinvestigation (with Subject Interview)	58	\$1,279	\$1,381
T3	Tier 3	64	\$440	Not Available
T3R	Tier 3 Reinvestigation	65	\$424	Not Available
T4	Tier 4	66	\$4,233	\$4,571
T4R	Tier 4 Reinvestigation	67	\$2,723	\$2,940
T5	Tier 5	70	\$5,706	\$6,163
T5R	Tier 5 Reinvestigation	71	\$3,134	\$3,385

Figure 2. National Background Investigations Bureau Projected Billing Rates FY 2019⁵²

⁵² Source: United States Office of Personnel Management, *FY 2019 Investigations Reimbursable Billing Rates Effective October 1, 2018* (Washington, DC: National Background Investigations Bureau, 2017), 1, <https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/2017/fin-17-05.pdf>.

Case Type		Case Type Code	Case Service	
			Standard	Priority
NAC	National Agency Check	06	\$160	Not Available
T1	Tier 1	63	\$199	Not Available
T2	Tier 2	55	\$563	\$608
T2R	Tier 2 Reinvestigation	56	\$267	\$288
T2S	Tier 2 (with Subject Interview)	57	\$1,584	\$1,711
T2RS	Tier 2 Reinvestigation (with Subject Interview)	58	\$1,288	\$1,391
T3	Tier 3	64	\$443	Not Available
T3R	Tier 3 Reinvestigation	65	\$427	Not Available
T4	Tier 4	66	\$4,263	\$4,604
T4R	Tier 4 Reinvestigation	67	\$2,742	\$2,961
T5	Tier 5	70	\$5,746	\$6,206
T5R	Tier 5 Reinvestigation	71	\$3,156	\$3,408

Figure 3. National Background Investigations Bureau Projected Billing Rates FY 2020⁵³

C. SECURITY CLEARANCE BACKLOG IMPACTS

The impact of the backlog of security clearance investigations has resulted in the addition of a government-wide security clearance process to the GAO’s high-risk list due to continued challenges associated with processing security clearance investigations within the timeline set by the IRTPA.⁵⁴ From 2014 to 2018, the backlog of investigations increased from approximately 190,000 to 710,000.⁵⁵ The GAO released a report on the Security Clearance Suitability, and Credentialing Performance Accountability Council. This council is a group comprised of the Deputy Director for Management, Office of Management and Budget; Suitability and Credentialing Executive Agent, U.S. Office of

⁵³ Source: National Background Investigations Bureau, United States Office of Personnel Management, “FY 2020 Initial Estimated Pricing,” 2018, <https://nbib.opm.gov/hr-security-personnel/investigations-billing-rates-resources/billing-rates/future-billing-rates/>.

⁵⁴ Government Accountability Office, *High Risk*, 1.

⁵⁵ Government Accountability Agency, *Testimony before the Select Committee on Intelligence, U.S. Senate, Personnel Security Clearances*, 1.

Personnel Management; Security Executive Agent, Office of the Director of National Intelligence; and the Under Secretary of Defense for Intelligence, Office of the Director of National Intelligence who are responsible for implementing reforms to security clearance issues.⁵⁶The GAO stated:

While the PAC has made progress reforming the security clearance process since the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), several critical areas of the reform effort—such as the implementation of continuous evaluation, and the issuance of a reciprocity policy—remain incomplete. Over the last nine years, we have made 43 recommendations to executive branch agencies to improve the personnel security clearance process; however, only 12 of them had been fully implemented as of January 2018.⁵⁷

The backlog of security clearances translates to an understaffed job market. A staffing recruiter for companies seeking candidates with security clearances, ClearJobs.com, interviewed a number of companies to get their feedback on the security clearance backlog. Employers' comments are grim to say the least. Interviewees responsible for hiring candidates with security clearances have noted, "This is just one more thing that makes it harder in the already extremely competitive market for fully-cleared professionals," and "Now, every contractor is at war, stealing each other's employees, and this is going to negatively impact our government customer."⁵⁸ Figure 4 depicts a sharp decrease in the number of currently employees with a security clearance. The lack of workers with a security clearance is a potential capability gap to supporting national security work.

⁵⁶ Government Accountability Office, *High Risk*, 1.

⁵⁷ Government Accountability Office, 1.

⁵⁸ "Security Clearance Trends," ClearJobs, accessed February 5, 2019, <https://about.clearancejobs.com/employers/security-clearance-trends/>.

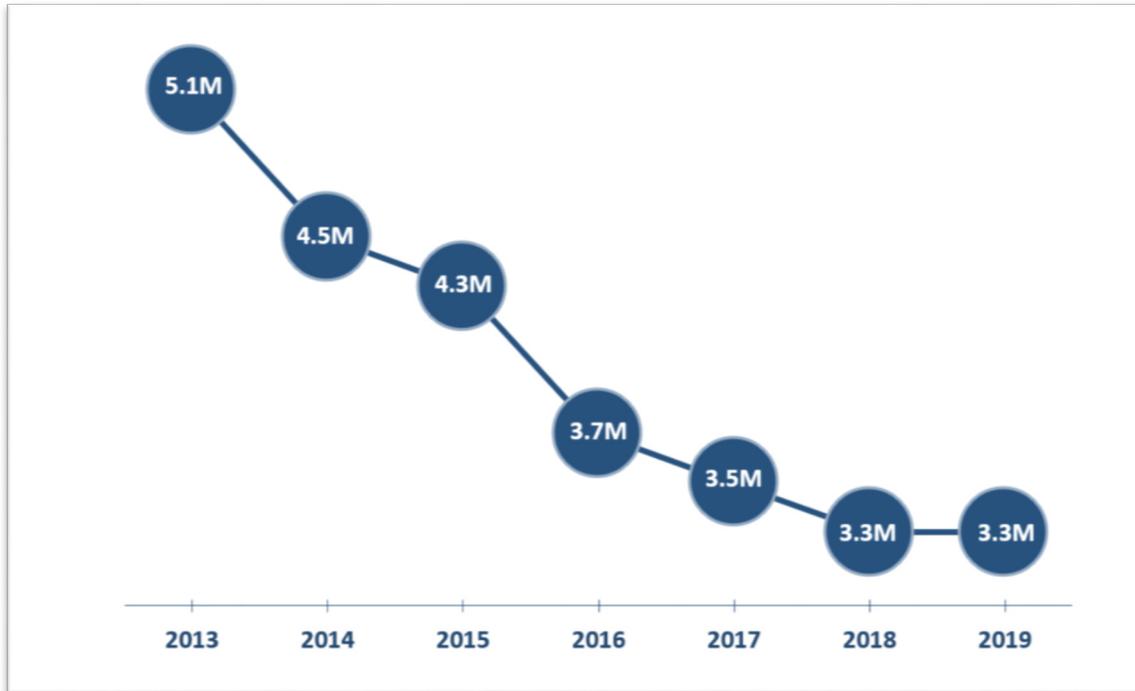


Figure 4. Security Clearance Population 2013–2019⁵⁹

The security clearance backlog may seem to be a problem that exists in governments across the world, but other countries have had more success with their timeliness standards. The Australian government issues security clearances to individuals to certify that they can be trusted with safeguarding sensitive information as part of their daily roles and responsibilities serving the government. Australia organizes its sensitive information classification into four categories: Baseline Vetting, Negative Vetting Level 1, Negative Vetting Level 2, and Positive Vetting.⁶⁰ Baseline Vetting is the least sensitive clearance while Positive Vetting is the most sensitive clearance.⁶¹ The Australian Government Security Vetting Agency (ASGVA) is responsible for completing the background investigation for most government agencies in the Australian intelligence

⁵⁹ Source: ClearanceJobs.

⁶⁰ “Clearance Subject FAQs,” Australian Government, Department of Defence, 1, February 6, 2014, <http://www.defence.gov.au/AGSVA/FAQ/clearance-subject.asp>.

⁶¹ Australian Government, Department of Defence, 1.

community with the exception of the following agencies: Department of Foreign Affairs, Australian Security Intelligence Organisation, Australian Federal Police, Australian Secret Intelligence Service, and the Office of National Assessments. Those agencies that do not rely on the ASGVA complete their own security clearance background investigations and adjudications.⁶²

The ASGVA's goals for completing investigations and adjudications of their clearances are one month for Baseline clearances, four months for Negative Vetting Level 1, six months for Negative Vetting Level 2, and six months for Positive Vetting.⁶³ The ASGVA processed approximately 47,471 security clearances between 2016–2017 and anticipated to process 47,970 security clearances between 2017–2018. Between 2015–2016, the average processing time for a baseline security clearance was 27.4 days.⁶⁴ While Baseline investigations are within the goal for timely completion set by the ASGVA, challenges have arisen in completing higher-level clearance investigations. At the peak of the Australian security clearance backlog, the most sensitive clearance holders could expect to wait up to 18 months to receive their completed security clearance.⁶⁵ While Australia has had challenges completing their most sensitive level clearance investigations and adjudications within their timeliness goals, it still manages to complete 55 percent of its security clearance investigations and adjudications within its timeline.⁶⁶

D. INFORMATION CLASSIFICATION TRENDS

The Information Security Oversight Office within the National Archives conducts annual reporting on trends in the fields of information security related to the U.S.

⁶² Australian Government, Department of Defence, 1.

⁶³ Australian Government, Department of Defence, 1.

⁶⁴ Sally Whyte, "The Govt's Plans to Slash Backlog of Security Clearances," *Sydney Morning Herald*, 1, June 25, 2018, <https://www.smh.com.au/politics/federal/the-govt-s-plans-to-slash-backlog-of-security-clearances-20180620-p4zmot.html>.

⁶⁵ Canberra ACT, *2017 Independent Intelligence Review* (Canberra ACT: Commonwealth of Australia, 2017), 77, <https://www.pmc.gov.au/sites/default/files/publications/2017-Independent-Intelligence-Review.pdf>.

⁶⁶ Kate Grayson, "Vetting the Veters," *The Strategist*, 1, August 14, 2017, <https://www.aspistrategist.org.au/vetting-the-veters/>.

government. In 2016, more information was declassified, and less novel information was classified.⁶⁷ Figures 5 and 6 illustrate the significant downward trend in these areas. While less novel information is being classified and more information is being declassified, it can be assumed that continuing the reduction in the security clearance population will be consistent with other trends in information security in the U.S. government. A possibility exists, however, that the security clearance population trends in the United States may operate independently of these trends. More people may have a need to know for the classified information shared between departments and agencies. One of the most scathing criticisms in the *9/11 Commission Report* was that agencies were not communicating effectively with one another and failed to share intelligence to see the larger big picture.⁶⁸

⁶⁷ “ISOO Reports,” National Archives, September 12, 2016, <https://www.archives.gov/isoo/reports>.

⁶⁸ Thomas H. Kean and Lee H. Hamilton, *The 9/11 Commission Report* (Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004), 417–418.

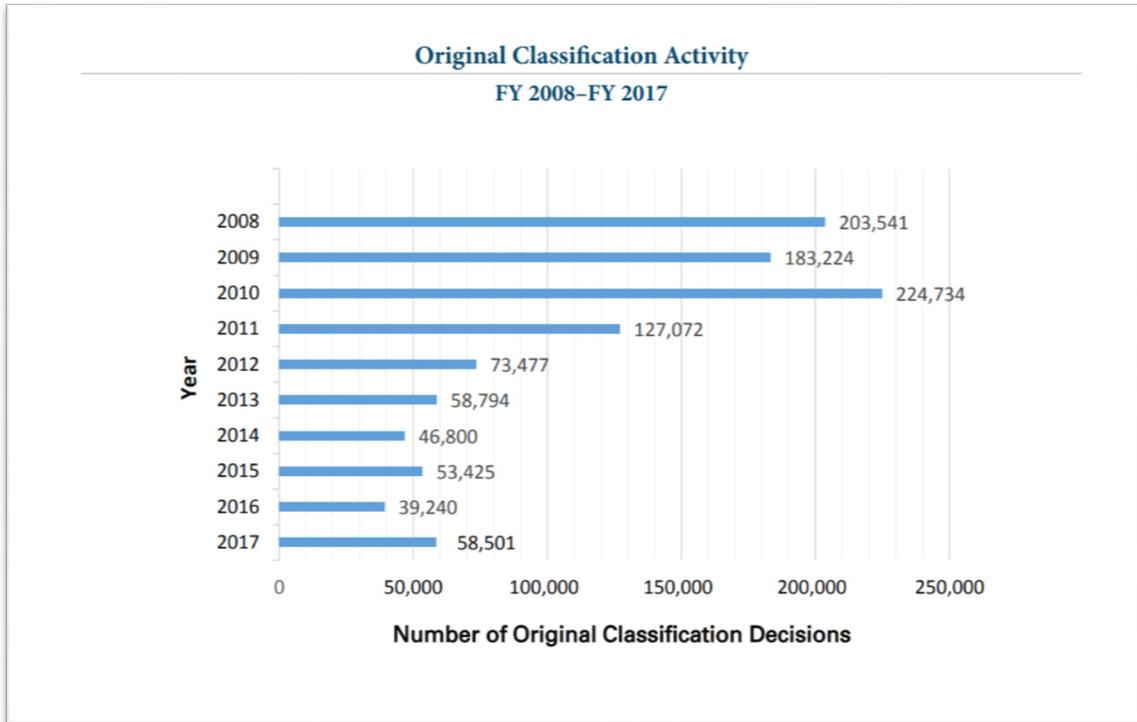


Figure 5. Original Classification Activity FY 2008–FY 2017⁶⁹

⁶⁹ Source: Information Security Oversight Office, *Report to the President 2017* (Washington, DC: National Archives and Records Administration, 2018), 42, <https://www.archives.gov/files/isoo/reports/2017-annual-report.pdf>.

Total Number of Pages Reviewed and Declassified*

FY 2008–FY 2017

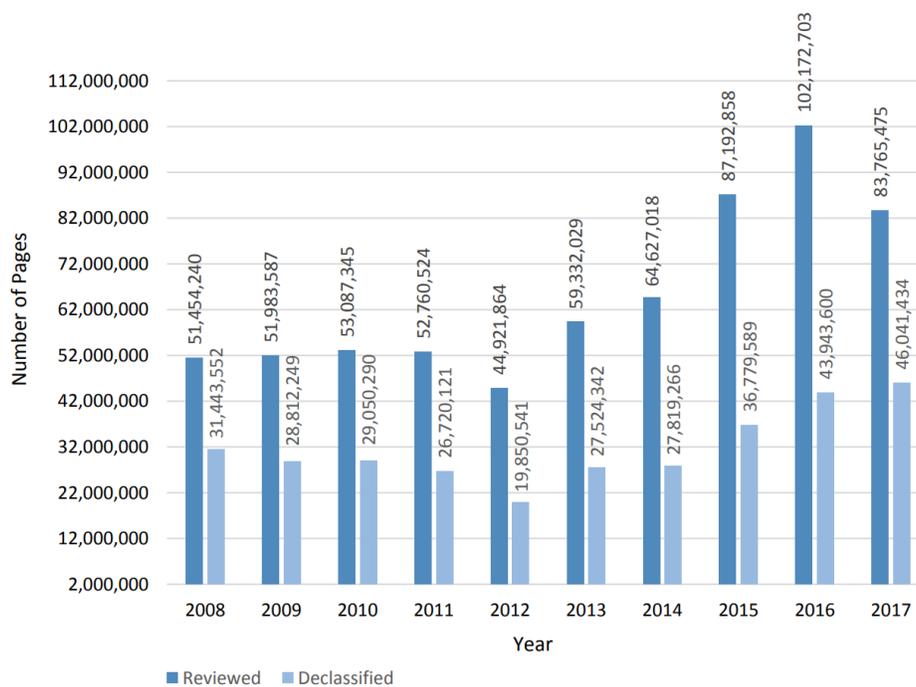


Figure 6. Total Number of Pages Reviewed and Declassified FY 2008–FY 2017⁷⁰

⁷⁰ Source: Information Security Oversight Office, 46.

III. POLICY OPTIONS REVIEWED

This chapter examines three policy options that could reduce the security clearance background investigation backlog. Policy options for consideration draw on academic concepts discussed in the literature review. The three proposed policy options to reduce the security clearance backlog are using the current process with the addition of continuous evaluation, hiring additional NBIB background investigator staff, and limiting the number of security clearance background investigations to the NBIB investigator staff annual throughput.

A. POLICY OPTION CRITERIA

Policy options will employ either a developmental, transitional, or transformational approach to organizational change. Presently, the NBIB is responsible for approximately over 90 percent of the security clearance background investigation workload. Thus, policies suggested will be for the use and consideration of the NBIB. It should be noted that with the looming reorganization of the NBIB and the transferring of background investigation roles and responsibilities back to the DOD for their staff, that these policy suggestions and approaches may only be altered slightly, but still recommended regardless of the reorganization status due to the large challenge that the security clearance backlog poses. For the purposes of the following recommendations, the author assumes that the NBIB will still maintain its current role and share of the investigation burden. Policy options suggested in this chapter will make improvements to the components of either information security, personnel security, or risk management principles. The best policy will make the most positive outcome gains in all areas and notionally decrease the security clearance background investigation backlog.

B. POLICY OPTION 1: CURRENT PROCESS WITH THE ADDITION OF THE CONTINUOUS EVALUATION DEVELOPMENTAL APPROACH

The current process for security clearance investigations and adjudications in the United States does not limit the number of clearances (whether in access or not in access) that a given agency has. If an agency deems that a position within its organization requires

a security clearance for its official duties, it pays for background investigations and reinvestigations for its employees and determines whether they are a security risk based on the results of its investigation.

The aforementioned approach utilizes information from the applicant reviewed by background investigators initially then reinvestigated periodically. This initial and periodic screening process ensures federal employees and contractors are suitable and trustworthy to access sensitive information and validates that they have not increased their risk factors throughout the course of their employment. Periodic re-investigations of individuals help keep sensitive information protected from insider threats to secure systems; however, depending on the type of security clearance an individual holds, the amount of time between reinvestigation may vary. The addition of annual continuous evaluation for all individuals with a security clearance would be a transitional approach to changing the way the NBIB conducts business. Since reinvestigations for individuals whom hold security clearances are already a part of the NBIB mission and scope, adjusting the frequency of reevaluation to make improvements to information security would be a logical improvement.

1. Policy Option 1 Benefits

The current strategy for ensuring information security within the security clearance population relies on vetting cleared individuals through security clearance reinvestigations, as well as vetting new candidates for security clearances during their initial background investigation. Individuals can be denied access to classified information prior to being hired to a sensitive position if they do not obtain a favorable background investigation. By screening out potential actors prior to access to sensitive information, information security can be achieved. What may be more concerning, however, is the large population of individuals with access to classified information who have the potential to disclose critical national security information. The added scrutiny of annual continuous evaluation will enable closer monitoring of individuals who have access to classified information and provide agency security personnel security officers the opportunity to interdict, or more closely monitor individuals who return negative information during their reinvestigation.

Annual reporting on security clearances shows how low the security clearance denial and revocation rates are in the United States.

The Office of the Director of National Intelligence releases annual reports on agency trends in security clearances. According to the 2017 Annual Report on Security Clearance Determinations, a number of security clearance denials resulted along with security clearance revocations.⁷¹ Table 1 depicts the number of revocations and clearance denials per agency. Among the 10 agencies analyzed, the average security clearance denial rate was 1.94 percent while the clearance revocation rate was 0.56 percent. No specific report information was available to determine the causes of agency security clearance denials and revocations or the reasons between the variance between agencies 1–10.

Table 1. ODNI Annual Report on Security Clearance Determinations Agency Security Clearance Denials and Revocations FY 2017⁷²

Agency	FY 2017	
	Denials	Revocations
Agency #1	5.6%	1.4%
Agency #2	0.0%	0.0%
Agency #3	5.9%	0.0%
Agency #4	2.6%	2.3%
Agency #5	0.2%	0.6%
Agency #6	0.2%	0.4%
Agency #7	0.2%	0.1%
Agency #8	4.6%	0.4%
Agency #9	0.1%	0.4%
Agency #10	0.0%	0.0%

⁷¹ National Counterintelligence and Security Center, *Fiscal Year 2017 Annual Report on Security Clearance Determinations* (Washington, DC: Office of the Director of National Intelligence, 2018), 8, <https://www.dni.gov/files/NCSC/documents/features/20180827-security-clearance-determinations.pdf>.

⁷² Source: National Counterintelligence and Security Center, 8,

The addition of annual continuous evaluation could serve as a mechanism to improve the state of information security of classified information in the United States. Providing as many opportunities as possible for the alerting of staff maladaptive behavior could allow for the removal of employees deemed no longer trustworthy and able to handle the responsibility of accessing classified information. Potential challenges associated with this proposed approach are outlined in the next subsection.

2. Policy Option 1 Challenges

One challenge of the current investigation and adjudication process is that it does not provide for the timely investigation adjudication of personnel. Figure 7, from the Security Clearance, Suitability, and Credentialing Performance Accountability Council (PAC), shows that since 2012, the time it takes to investigate individuals for both Secret and Top Secret security clearances has been increasing.



Figure 7. Average Timeliness for Processing the Fastest 90 Percent of Security Clearance Cases⁷³

Additional PAC data suggest that FY 2018 has the highest projected security clearance background investigations and reinvestigations that are both of high and low field work intensity. Cases with low fieldwork intensity involve automated system checks while high field intensity investigations involve manual checking of information provided by the applicants, which is more common for positions with higher sensitivity. Figure 8 depicts the increase in the number of investigations and reinvestigations that require more fieldwork, which translates to longer overall investigation times for individuals.

⁷³ Source: “Security Clearance, Suitability, and Credentialing Reform,” General Services Administration & the Office of Management and Budget, accessed October 12, 2018, https://www.performance.gov/CAP/CAP_goal_13.html.

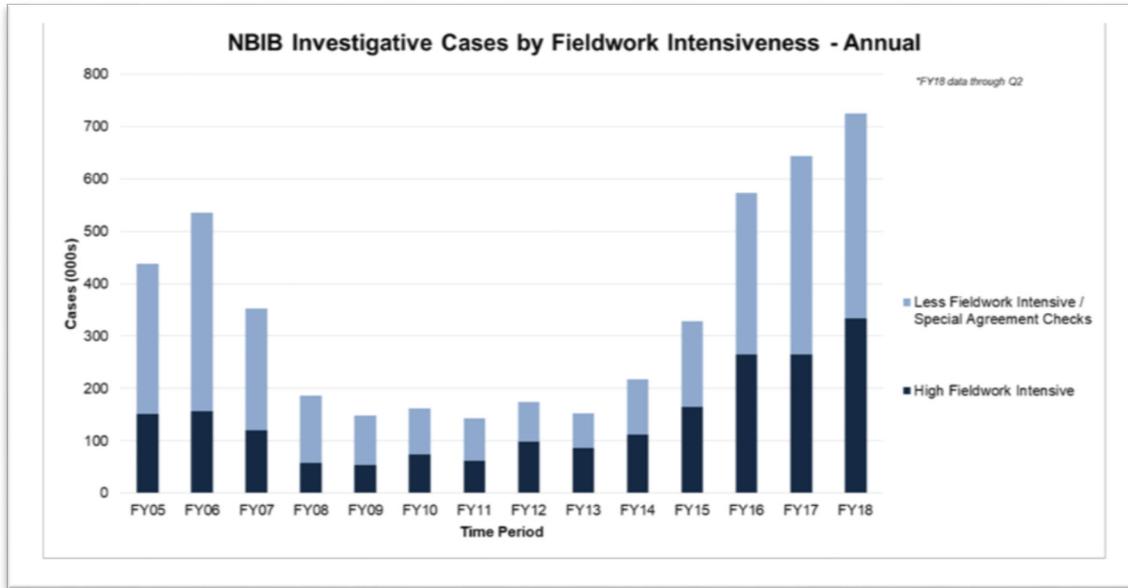


Figure 8. National Background Investigations Bureau Investigation Fieldwork Intensiveness FY 2005–FY 2018⁷⁴

The increasing length of time spent on background investigation of employees and contractors has not guaranteed the security of sensitive and classified information. Two major security breaches by individuals with security clearances occurred between 2010 and 2015. In 2010, Chelsea (then-Bradley) Manning, an intelligence analyst for the United States Army, leaked classified information to the public concerning detainee treatment during the war in Iraq.⁷⁵ Three years later, Edward Snowden, an NSA contractor, leaked classified information to the press regarding a classified information collection program. Unfortunately, sensitive information leaks are just one aspect of concern in the realm of personnel and information security. In 2013, Major Nidal Hassan killed 13 people in Fort Hood, Texas. In September 2013, Aaron Alexis killed 12 people at the Navy Yard in Washington, DC.⁷⁶ Both individuals held Secret security clearances. Even if individuals are deemed trustworthy to safeguard national security information, the aforementioned

⁷⁴ Source: General Services Administration & the Office of Management and Budget.

⁷⁵ Lanktree, “Leaker Chelsea Manning Reveals for the First Time Why She Released Secret Military and Diplomatic Documents.”

⁷⁶ Department of Defense, *Internal Review of the Washington Navy Yard Shooting*, 11.

examples serve as a grave reminder of the importance of continually re-evaluating holders of security clearances. Adding continuous evaluation to the current security clearance process may increase the overall workload on the NBIB staff. If the entire security clearance population had to be reinvestigated on an annual basis, more staff time would have to be allotted to achieve this task. The gains in information and personnel security would have to be weighed against the tradeoffs of added time to the security clearance process.

3. Policy Option 1 Outcome Assumptions

The assumed outcomes of the current process are security clearance background investigations not meeting IRTPA timeliness standards, but are succeeding in providing some safeguards to sensitive information integrity because of working policies that result in security clearance revocations and denials. By taking a developmental approach to the current organization of the NBIB, it could be argued that adding a requirement for all holders of a security clearance to be continuously evaluated would be within scope of the functions that the NBIB already performs. While this additional requirement across the population of security clearance holders would undoubtedly add to the length of time and the workload of current background investigators, automated systems exist that could lessen the burden of work on the individual investigator. The DOD employs an automated system named the Automated Continuous Evaluation System (ACES) to monitor their employees' eligibility to access classified information.⁷⁷ According to the DOD, the current configuration of ACES allows for point in time checks against verified systems; however, future iterations of the system will enable relevant records to be pushed to it to allow for updates without human intervention.⁷⁸

⁷⁷ "Initiatives: Automated Continuous Evaluation System (ACES)," Department of Defense, Defense Human Resources Activity, accessed December 7, 2018, <https://www.dhra.mil/PERSEREC/Initiatives/#ACES>.

⁷⁸ Office of Freedom of Information, *Report on DoD Plans to Adopt Continuous Evaluation (CE) and Insider Threat Capabilities* (Washington, DC: Department of Defense, 2015), 7, <https://fas.org/sgp/othergov/dod/ce-2015.pdf>.

In adding the continuous evaluation requirement across the entire clearance population, an assumption would be that using a National Agency Check would be considered adequate to catch the majority of factors that should disqualify individuals from accessing classified information. Looking at the current investigation rates of the NBIB, note that a National Agency Check costs approximately \$154. This cost across the entire clearance population annually would equate to \$471,240,000 (90 percent multiplied by the approximately 3.4 million security clearance population). Since the agency hiring candidates with security clearance pays the NBIB for the background investigation services, it is assumed that this cost would be divided among the agencies that rely on the NBIB for background investigations.

The developmental approach previously described; i.e., a continuous evaluation process, would increase information security by ensuring the individuals within the security clearance population were still trustworthy and able to access classified information safely. Depending upon the technology employed, this process could either increase or decrease the backlog of security clearance investigations. It is not assumed that the next generation of the DOD ACES previously described is currently operational. Thus, this approach would lengthen the security clearance backlog by increasing the workload of NBIB investigators. The continuous evaluation requirement would not necessarily improve the quality of initial investigations; however, it could be argued that this type of evaluation would increase the quality of reinvestigations by allowing increased verification of personnel within the security clearance population. The aforementioned approach would make incremental improvements in information security outcomes. However, the increased cost of implementing this option may deter policy makers.

C. POLICY OPTION 2: INCREASE THE NUMBER OF NATIONAL BACKGROUND INVESTIGATIONS BUREAU INVESTIGATORS TRANSITIONAL APPROACH

Increasing the NBIB staff investigator capacity is a potential option that may reduce the backlog of security clearance investigations and also potentially increase the quality of background investigations and reinvestigations for security clearances. This transitional approach to organizational change in the NBIB could allow for a phased approach to

onboarding new staff and building investigation capacity that would result in an organizational transition to a new, more efficient environment. The current number of investigators working for the NBIB, which handles 90 percent of the workload for security clearance background investigations, is 7,200.⁷⁹

An analysis of NBIB staffing reveals how challenging the task of clearing the investigation backlog of approximately 639,000 investigation products (90 percent of the 710,000 investigation product backlog). The following equation shows 90 percent of the backlog of investigation products divided by the number of investigators who work at the NBIB. It should be noted that this calculation illustrates a snapshot of investigation products at the height of the security clearance backlog and does not account for the continued addition of novel investigations or reinvestigation products.

$$\frac{639,000 \text{ investigation products}}{7,200 \text{ investigators}} = 88.75 \text{ cases per investigator}$$

The metric established by the Intelligence Reform and Terrorism Prevention Act of (IRPTA) of 2004 is for all government agencies to complete 90 percent of their security clearance investigations within 60 days. This agency requirement is missed year after year and has resulted in delays for individuals starting their new national security position or maintaining access to classified information with their current positions. In a given work year, 261 working days (2,088 work hours) are assumed, which accounts for the subtraction of weekends and federal holidays. To clear just the security clearance backlog (not considering new investigations or reinvestigations) in a year's time, NBIB investigators can theoretically spend only 23.5 hours per backlog case. If NBIB investigators were being held to strict IRTPA timeliness standards, they would spend only 5.41 hours on a single investigation.

$$\frac{2,088 \text{ working hours (261 working days in a year)}}{88.75 \text{ cases per investigator}} = 23.53 \text{ hours per investigation}$$

⁷⁹ United States Office of Personnel Management, *Statement of Charles S. Phalen, Jr.*, 2.

480 working hours (60-day ITRPA requirement) = 5.41 hours per investigation
88.75 cases per investigator

It is clear that the amount of time that NBIB investigators realistically have to work on background investigations is limited. If background investigators only spent 5.41 hours per investigation regardless of its sensitivity, it is logical to assume that the quality of the investigation will suffer dramatically. It is assumed that since the NBIB does not want to sacrifice the quality of its investigations over the timeliness standards set forth in the ITRPA, investigations are taking years to complete instead of months.

However, according to Charles Phalen, director of the NBIB, the current security clearance investigation backlog of 710,000 is misleading because the caseload in which the NBIB can meet ITRPA timeliness requirements is 160,000–180,000 investigations.⁸⁰ When assuming that Phalen’s statement reflects that the 160,000 investigation product workload may be manageable for current NBIB staff and provide the amount of time per investigation may result in a quality investigation outcome, how much additional time will be added per case can be seen in the following equations:

160,000 investigation products = 22.2 cases per investigator
7,200 investigators

2,088 working hours (261 days in a year) = 94.05 hours per case
22.2 cases

480 working hours (60-day ITRPA requirement) = 21.81 hours per case
22.2 cases

The ideal investigation workload distributed the current NBIB staff allows for significantly more time per investigation product and would logically increase the quality of investigations and reinvestigations. While it is good to know what an ideal workload would be for NBIB investigators that would theoretically result in quality investigations,

⁸⁰ United States Office of Personnel Management, *Statement of Charles S. Phalen, Jr., 2.*

action could still be taken on the surplus of security clearance investigations and reinvestigations that exist in the United States.

1. Policy Option 2 Benefits

Increasing the investigator capacity for the NBIB would preserve quality investigations while reducing the security clearance backlog. Assuming that the ideal investigation workload per investigator is 22.2 cases, a staff of approximately 29,045 investigators (four times the current staffing) would be required to clear the security clearance backlog in one year's time. This number would not account for novel background investigations or reinvestigations of current security clearance holders.

639,000 investigation products = 29,045 investigators

22.2 cases per investigator

2,088 working hours (261 working days) = 94.05 hours per case

22.2 cases per investigator

480 working hours (60-day IRPTA requirement) = 21.81 hours per case

22.2 cases per investigator

Even in an ideal workload, the amount of time that each investigator has to work on a case in a given year is limited. As of 2017, the total security clearance population in the United States is 4,030,625. This large population of clearance holders may benefit from additional investigator staff to check continually that individuals who have access to classified information are still trustworthy and do not pose a risk to the security of the nation.

2. Policy Option 2 Challenges

The challenge to this approach is that it is potentially cost burdensome. Adding the approximately 21,000 additional investigators required to address the security clearance backlog in a timely manner may be cost prohibitive. Even if additional funds required to hire the additional investigator staff was not an issue, the amount of time required to train

and integrate these staff would potentially be a slow process. Ensuring that quality investigators are performing background investigations is critical for maintaining quality of the overall background investigations and reinvestigations.

3. Policy Option 2 Outcome Assumptions

Hiring additional investigators will decrease the security clearance backlog. While a decrease in the security clearance backlog would help fill the number of critical positions left vacant by the backlog, this approach alone would not significantly improve security conditions for individuals with access to classified information. More clearance holders could mean a higher risk for insider threats and security breaches, but a greater potential to share information would exist among trusted clearance holders with this approach.

D. POLICY OPTION 3: LIMIT CLEARANCE POPULATION TO INVESTIGATOR THROUGHPUT TRANSFORMATIONAL APPROACH

A transformational approach to organizational change within the NBIB would be to limit the number of security clearance investigations and reinvestigations per year to the number of investigations and or reinvestigations the NBIB could process while maintaining a quality outcome for security clearance investigations. This approach would be an environment of significant change for the NBIB. Currently, the number of investigation products that the NBIB can support through its services is unlimited. This approach would also notionally strain any novel positions added to the national security enterprise.

This approach may seem daunting considering the current population of security clearance holders. The number of federal employees and contractors who hold security clearances in the U.S. government is 4,030,625. Employees and contractors who hold security clearances can be divided into two major categories, in access, and eligible, not in access. In access refers to individuals actively accessing classified information. Eligible, not in access, refers to individuals eligible to access classified information, but who do not

currently access it in the course of their duties. Figures 9 and 10 show the clearance population distribution from 2017.⁸¹

As of 10/1/17:	
Conf/Secret	Top Secret
1,636,979	1,194,962
2,831,941	

Figure 9. Eligible, in Access Population CY 2017⁸²

As of 10/1/17:	
Conf/Secret	Top Secret
1,083,853	114,831
1,198,684	

Figure 10. Eligible, Not in Access CY 2017⁸³

As discussed earlier, it is known that the ideal caseload for NBIB investigations is approximately 160,000–180,000 investigations per year. If this approach were selected, it would mean that the combination of novel investigation and reinvestigations would not be

⁸¹ National Counterintelligence and Security Center, *Fiscal Year 2017 Annual Report on Security Clearance Determinations*, 5.

⁸² Source: National Counterintelligence and Security Center, 5.

⁸³ Source: National Counterintelligence and Security Center, 5.

able to exceed the 160,000–180,000 case range. It should be noted, however, that not all investigations require the same amount of time to complete. Within the security clearance investigation backlog, 340,000 are initial investigations, 206,000 are periodic investigations, and 164,000 are automated record checks.⁸⁴ As shown in Figure 11, using that metric as a baseline and a trend in the distribution of investigations overall, it would be assumed that 48 percent of future clearances could potentially be new hires, 29 percent would be reinvestigations with the remainder of automated record checks making up 23 percent. Unfortunately, the type of investigation that theoretically takes the least amount of time for an investigator to perform (the automated record check) accounts for the least amount of the security clearance backlog.

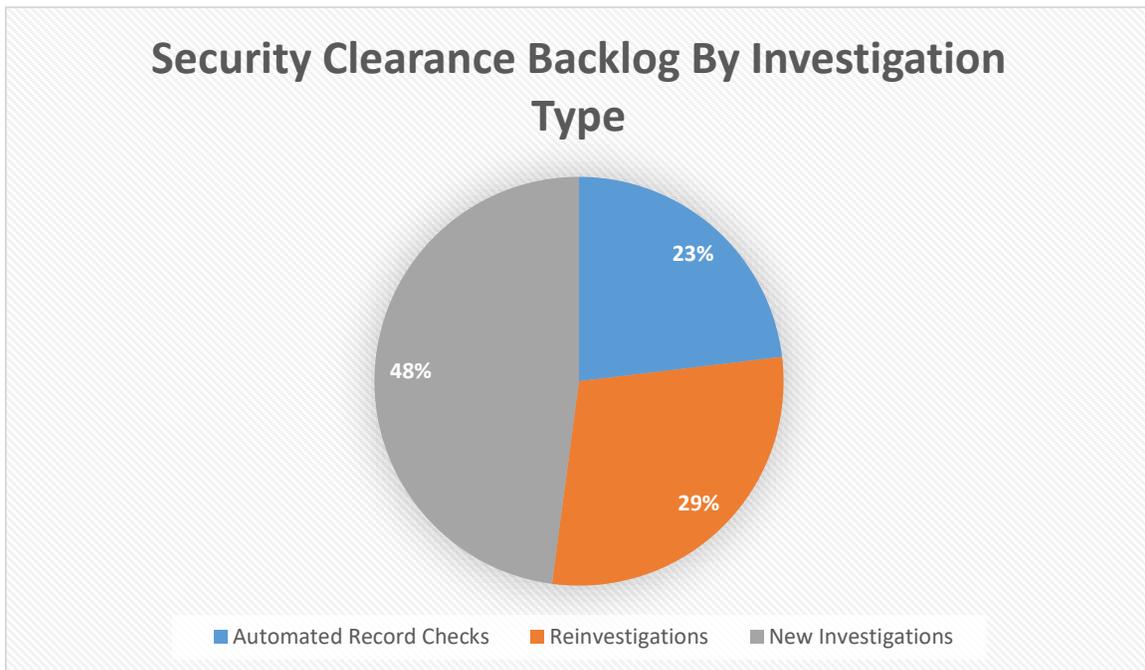


Figure 11. Security Clearance Investigation Backlog by Investigation Type

In the new proposed environment that limited the number of clearances processed to the throughput of the NBIB investigator capacity (160,000–180,000 investigations), this

⁸⁴ United States Office of Personnel Management, *Statement of Charles S. Phalen, Jr.*, 2.

process would mean that the new clearance investigations would be limited to approximately 76,000–86,400, reinvestigations would account for 46,000–52,000, and automated checks would account for 36,800–41,400. This new normal is 23–25 percent of the current backlog, and may make departments and agencies that rely on the NBIB’s investigation services concerned since a re-prioritization of positions will undoubtedly have to occur with security clearances government wide to accompany this strategy.

When trying to determine where to start with the government re-prioritization of positions with security clearances, the population currently eligible, not in access, may be a good starting point. Prioritizing the current capacity of background investigators to focus their initial and periodic reinvestigation resources on those who are or will be in access may allow individuals who need to work with classified information to be more prioritized for minimal impacts to work that needs individuals to have frequent secure access. As a long-term solution, the eligible, not in access clearance population, should be reduced as much as possible to free up investigation resources for the eligible in access clearance population.

1. Policy Option 3 Benefits

Limiting the number of security clearance investigations to the investigation throughput of the NBIB would notionally increase the investigation quality, reduce the backlog of security clearances (assuming the NBIB was allowed to cease novel investigations and focus on reducing the backlog), increase the security of national security information, and result in no additional costs to the current security clearance investigation process. The quality of security clearance investigations would increase because NBIB investigators would have more time to spend per investigation. The security clearance investigation backlog could be reduced in just over four years (assuming this change in policy froze novel investigations, $710,000/160,000 = 4.4$). Information security of national security information would be increased by reducing the number of individuals with access; fewer people reduce the chances for insider threat. Finally, costs would not increase by adopting this approach since no new staff would be required.

2. Policy Option 3 Challenges

Sharing sensitive and classified information between agencies is essential to breaking down stove piping between agencies that can lead to catastrophic consequences.⁸⁵ When the number of individuals with access to national security information across agencies decreases, reduced collaboration is also possible. Limiting the population with access to sensitive information increases the potential for negative impacts to the ability for the U.S. government to collaborate in the homeland and national security mission. Assuming that the number of security clearance initial investigations is a trend that is likely to continue and due to the demand of new positions being created that require security clearances, it can be assumed that pushback will result from the national security community relying on the NBIB for background investigation support. It can be argued that limiting the number of security clearances to the investigation throughput of the NBIB limits the capabilities of the national security enterprise to perform its essential work. This assumption could be countered by stating this number would be offset in a relatively short amount of time once the backlog was eliminated. Agencies are already waiting over a year or more for security clearances in some cases. Thus, this approach, if it resulted in fixing the overall problem, may be acceptable.

3. Policy Option 3 Outcome Assumptions

As noted previously, limiting the number of investigations to NBIB's throughput assumed that in addition, the NBIB could freeze accepting novel investigations. It is also assumed that the reduction of the clearance security clearance population is consistent with an ongoing trend in the reduction of the overall clearance population. The population of individuals with a security clearance between October 2016 and October 2017 decreased. The eligible, in access population decreased by 0.3 percent, while the eligible, not in access decreased by 3.4 percent.⁸⁶ Between 2015 and 2016, the clearance population also decreased. The eligible, in access population decreased by 0.9 percent, while the eligible,

⁸⁵ Kean and Hamilton, *The 9/11 Commission Report*, 417–418.

⁸⁶ National Counterintelligence and Security Center, *Fiscal Year 2017 Annual Report on Security Clearance Determinations*, 5.

not in access population decreased by 10.3 percent.⁸⁷ This percentage is consistent with other national security information classification trends across the U.S. government. More information is being declassified and the security clearance population is decreasing year to year.

⁸⁷ National Counterintelligence and Security Center, *2016 Security Clearance Determination Report* (Washington, DC: Office of the Director of National Intelligence, 2017), 5.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FINDINGS

Next, the aforementioned detailed policy options are compared against each other and scored to determine which policy has the potential to make the most improvements in the security clearance backlog while preserving information security. The following method was created to score each approach based on positive and negative consequences on the security clearance backlog, as well as the integrity of information security. Policy options are summarized and then given a numerical score associated with factors that help improve or degrade the state of the security clearance investigation backlog and security of national security information. Each categorical rating within this methodology is weighted the same (for example, reducing the investigation backlog is equally important to maintaining information system security).

A. DEVELOPMENTAL APPROACH—ADDING ANNUAL CONTINUOUS EVALUATION TO THE CURRENT SECURITY CLEARANCE PROCESS

The developmental approach to changing how the NBIB currently conducts background investigations consists of adding a requirement to run national agency checks on holders of security clearances annually. This approach expands on how the NBIB currently conducts investigations, improves the quality of investigations, and maintains the integrity of national security information by validating that users with access are trustworthy. This approach would not reduce the security clearance backlog, nor would it reduce costs associated with background investigations.

B. TRANSITIONAL APPROACH—HIRING ADDITIONAL BACKGROUND INVESTIGATORS

The transitional approach to organizational change within the NBIB focuses on increasing investigator capacity by hiring additional investigators. This approach would bring the NBIB into an environment in which it would be able to meet the current demands for security clearance investigations, make improvements in information security and investigation quality, and reduce the security clearance backlog. This approach would also result in an increase in cost to the security clearance process, since the NBIB would have

to increase its staff from 7,200 to approximately 29,000 to keep up with demand and reduce the security clearance backlog.

C. TRANSFORMATIONAL APPROACH—LIMITING ANNUAL INVESTIGATIONS TO NBIB THROUGHPUT

Limiting the annual security clearance investigations to the throughput that the NBIB could still manage, as well as maintain quality investigations and would transform the operating environment for the NBIB, as well as for departments and agencies that rely on the NBIB for investigation support. This approach would reduce the backlog of security clearances over time, improve information security, and increase the quality of background investigations. This approach would not result in cost increases to the security clearance process.

Table 2 shows that the transformational approach to change within the NBIB may notionally result in the most improvements. Limiting the number of investigations and reinvestigations to NBIB investigation throughput, can possibly reduce the security clearance investigation backlog, increase the quality of investigations, as well as increase information security. While this policy option is not without its flaws, it is suggested that these large changes in policy may be required to make a significant impact on the compounding issues associated with the backlog of security clearance investigations and reinvestigations.

Table 2. Policy Option Comparison Model

	Does policy reduce security clearance investigation backlog? If so add 1 point.	Does policy improve information security? If so, add 1 point.	Does policy increase potential costs to security clearance process? If so, subtract 1 point.	Does policy increase quality of investigation? If so, add 1 point.	Total
Adding Annual Continuous Evaluation to the Current Security	+/-0	+1	+/-0	+1	2

	Does policy reduce security clearance investigation backlog? If so add 1 point.	Does policy improve information security? If so, add 1 point.	Does policy increase potential costs to security clearance process? If so, subtract 1 point.	Does policy increase quality of investigation? If so, add 1 point.	Total
Clearance Process					
Hire Additional Background Investigators	+1	+/-0	-1	+1	2
Reduce Clearance Population to Investigator Throughput	+1	+1	+/-0	+1	3

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. BEST POLICY

Based on the analysis, limiting the clearance population to the background investigator throughput achieves the best total positive outcome in the security clearance process. This policy option decreases the backlog by reducing the demand of investigations on security clearance investigators. Positive outcomes are gained in the quality of investigation by allowing investigators to take more time on their investigation products since they will have a sharply decreased caseload. This policy option also has the potential to improve information security by decreasing the number of individuals with access to classified information; the fewer individuals with access, the lower the chances are for system breaches by insider threat.

B. LIMITING FACTORS

Limiting the number of security clearance investigations to the throughput of the NBIB would require cooperation from the national security community. To catch up and eliminate the backlog, new investigations would have to be put on hold. This delay could frustrate approximately 100 agencies that rely on the NBIB for assistance in completing background investigations and reinvestigations for their staff. Without the support of the national security community, this policy would likely be unsuccessful.

C. IMPLEMENTATION CHALLENGES

The challenge to this transformational approach to addressing this problem is that the potential capacity to complete work in the homeland defense and national security space becomes limited. Cutting the number of individuals supporting homeland security and national defense missions without a phased approach could result in inadequate staffing to complete related missions. The limitation to fixing the number of cleared population to investigator capacity is that a significant amount of time will be required to develop staffing and workload transition plans to adapt to this new environment.

The potential of a limited capability of staff to share sensitive and classified information between the interagency also exists. While reducing the population with security clearances helps reduce the amount of threats that can impact sensitive information, it may limit the ability of the U.S. government to complete its national defense and homeland security mission.

D. SUGGESTIONS FOR FUTURE RESEARCH

The GAO 2017 report on security clearance reform (GAO-18-29) identifies specific areas that the U.S. government can improve upon to address the security clearance investigation backlog. Highlighted areas that may make a significant reduction in the security clearance investigation backlog include developing staffing plans to increase investigator capacity, developing a government-wide approach to reducing the backlog, and keeping data on and developing an implementation plan for security clearance reciprocity. This thesis has covered areas considered by the author to have the most impact if addressed. It is recognized, however, that security clearance reciprocity is an area that needs to be addressed to improve conditions contributing to the improvement of challenges related to security clearances.

Having data on the frequency of security clearance reciprocity government wide will help identify opportunities for leveraging the large population of individuals with security clearances to fill gaps in positions for which they are qualified. If clearance reciprocity were applied more consistently government wide, those investigations would potentially no longer add to the investigation backlog.

Beyond the GAO recommendations, it is recommended that agencies collect information on their experience with the background investigation and adjudication process so that critical paths can be identified and improved to reduce the overall time required to complete an investigation and adjudication. The *2015 ODNI Report on Security Clearance Determinations* provides some insight into the areas in which process improvements can be made that can reduce the backlog. Figure 12 shows that administrative errors accounted for the majority of significant delays to individuals in background investigations. Administrative errors could potentially be mitigated against

with clearer instructions for applicants and investigators, or forms or systems that rejected submissions due to inconsistencies. Documenting investigation experiences by agency could potentially aid in the identification of trend and root cause analysis.

Causes of Significant Delays																			
Agency	Volume			Delays															
	Government	Contractor	Total (Gov. + Cont.)	Multiple Issues	Administrative Matters	Other*	Significant Adjudicative Events							Misuse IT Systems					
ASP & ISP							Allegiance to U.S.	Foreign Influence	Foreign Preference	Sexual Behavior	Personal Conduct	Financial Considerations	Alcohol Consumption		Drug Involvement	Emotional / Mental	Criminal Conduct	Security Violations	Outside Activities
CIA	260	516	776	Unable to provide at this time															
DIA	376	0	376	0	376	0	0	0	0	0	0	0	0	0	0	0			
FBI	156	32	188	75	34	3	1	30	1	0	27	9	2	2	2	1	0	0	1
NGA	11	29	40	30	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0
NRO	2	160	162	0	0	69	0	20	0	0	3	26	15	12	1	16	0	0	0
NSA	140	519	659	515	22	11	0	67	0	0	6	20	5	3	2	8	0	0	0
State	118	28	146	97	0	25	0	19	1	0	1	3	0	0	0	0	0	0	0

* Other: Includes delays involving high risk cases, derogatory information, protected information, and polygraph or medical issues.

Figure 12. Causes of Security Clearance Investigation Delays⁸⁸

This thesis has analyzed factors contributing to the backlog of security clearance investigations and reinvestigations. Relevant literature in the fields of physical security, information security, risk management, and organizational change were surveyed to determine which appropriate academic concepts to employ to solve the problem. Policy options were developed for the NBIB and compared to determine how the most positive change could be made to achieve the outcome of reducing the security clearance investigation backlog while preserving information security. Through a comparative policy analysis, it was determined that the transformational approach of limiting the number of

⁸⁸ Source: National Counterintelligence and Security Center, *2015 Annual Report on Security Clearance Determinations*, 12.

background investigations to the throughput of the NBIB would successfully reduce the security clearance investigation backlog while preserving information security.

LIST OF REFERENCES

- Canberra ACT. *2017 Independent Intelligence Review*. Canberra ACT: Commonwealth of Australia, 2017. <https://www.pmc.gov.au/sites/default/files/publications/2017-Independent-Intelligence-Review.pdf>.
- Christenson, Michelle. *Security Clearance Process: Answers to Frequently Asked Questions*. CRS Report No. R43216. Washington, DC: Congressional Research Service, 2016. <https://fas.org/sgp/crs/secrecy/R43216.pdf>.
- Claycomb, William R., Carly L. Huth, Lori Flynn, David M. McIntire, and Todd B. Lewellen. "Chronological Examination of Insider Threat Sabotage: Preliminary Observations." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 3, no. 4 (December 2012): 4–20. <http://isyu.info/jowua/papers/jowua-v3n4-1.pdf>.
- ClearanceJobs. "Security Clearance Trends." Accessed February 5, 2019. <https://about.clearancejobs.com/employers/security-clearance-trends/>.
- Cunliffe, Ann L., and John T. Luhman. "Organizational Change." In *SAGE Key Concepts Series: Key Concepts in Organization Theory—Credo Reference*, edited by Ann L. Cunliffe and John T. Luhman, 111–117. London: Sage, 2013. https://search.credoreference.com/content/entry/sageukot/organizational_change/0.
- Department of Commerce. *Guide for Applying the Risk Management Framework to Federal Information Systems a Security Life Cycle Approach*. Rev. 1. Gaithersburg, MD: Department of Commerce, 2010. <https://permanent.access.gpo.gov/lps121083/sp800-37-rev1-final.pdf>.
- Department of Defence. Australian Government. "Clearance Subject FAQs." February 6, 2014. <http://www.defence.gov.au/AGSVA/FAQ/clearance-subject.asp>.
- Department of Defense. Defense Human Resources Activity. "Initiatives: Automated Continuous Evaluation System (ACES)." Accessed December 7, 2018. <https://www.dhra.mil/PERSEREC/Initiatives/#ACES>.
- . *Internal Review of the Washington Navy Yard Shooting*. Washington, DC: Department of Defense, 2013.
- General Services Administration & the Office of Management and Budget. "Security Clearance, Suitability, and Credentialing Reform." Accessed October 12, 2018. https://www.performance.gov/CAP/CAP_goal_13.html.

- Government Accountability Office. *High Risk: Government-Wide Personnel Security Clearance Process*. GAO-17-317. Washington, DC: Government Accountability Office, 2017. https://www.gao.gov/highrisk/govwide_security_clearance_process/why_did_study.
- . *Testimony before the Select Committee on Intelligence, U.S. Senate, Personnel Security Clearances, Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations Statement of Brenda S. Farrell, Director, Defense Capabilities and Management*. GAO-18-431T. Washington, DC: Government Accountability Agency, 2018. <https://www.intelligence.senate.gov/sites/default/files/documents/os-bfarrell-030718.pdf>.
- Grayson, Kate. “Vetting the Veters.” *The Strategist*, August 14, 2017. <https://www.aspi-strategist.org.au/vetting-the-veters/>.
- Hubbard, Douglas W. *The Failure of Risk Management: Why it’s Broken and How to Fix it*. Hoboken, NJ: Wiley, 2009.
- Information Security Oversight Office. *Report to the President 2017*. Washington, DC: National Archives and Records Administration, 2018. <https://www.archives.gov/files/isoo/reports/2017-annual-report.pdf>.
- Janczewski, Lech J., and Andrew M. Colarik. *Managerial Guide for Handling Cyber-Terrorism and Information Warfare*. Hershey, PA, Idea Group Publishing, 2005. <https://doi.org/10.4018/978-1-59140-583-2.ch001>.
- Kean, Thomas H., and Lee H. Hamilton. *The 9/11 Commission Report*. Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004.
- Kerber, Kenneth, and Anthony F. Buono. “Rethinking Organizational Change: Reframing the Challenge of Change Management.” *Organization Development Journal; Chesterland* 23, no. 3 (Fall 2005): 23–38.
- Kramer, Lisa A. *Technological, Social and Economic Trends that Are Increasing U.S. Vulnerability to Insider Espionage*. Technical Report Number 05-10. Monterey, CA: Defense Personnel Security Research Center, 2005. <https://fas.org/sgp/othergov/dod/insider.pdf>.
- Lanktree, Graham. “Leaker Chelsea Manning Reveals for the First Time Why She Released Secret Military and Diplomatic Documents.” *Newsweek*, June 9, 2017. <https://www.newsweek.com/chelsea-manning-interview-reveals-why-she-leaked-secret-military-documents-623668>.
- National Archives. “ISOO Reports.” September 12, 2016. <https://www.archives.gov/isoo/reports>.

- National Background Investigations Bureau. United States Office of Personnel Management. “Billing Rates.” Accessed December 4, 2018. <https://nbib.opm.gov/hr-security-personnel/investigations-billing-rates-resources/billing-rates/>.
- . “FY 2020 Initial Estimated Pricing.” 2018. <https://nbib.opm.gov/hr-security-personnel/investigations-billing-rates-resources/billing-rates/future-billing-rates/>.
- National Counterintelligence and Security Center. *2015 Annual Report on Security Clearance Determinations*. Washington, DC: Office of the Director of National Intelligence, 2016. <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2016/item/1603-2015-annual-report-on-security-clearance-determinations>.
- . *2016 Security Clearance Determination Report*. Washington, DC: Office of the Director of National Intelligence, 2017.
- . *Fiscal Year 2017 Annual Report on Security Clearance Determinations*. Washington, DC: Office of the Director of National Intelligence, 2018. <https://www.dni.gov/files/NCSC/documents/features/20180827-security-clearance-determinations.pdf>.
- Nextgov. “The Security Clearance Process Is About to Get Its Biggest Overhaul in 50 Years.” Accessed March 9, 2019. <https://www.nextgov.com/cio-briefing/2019/02/security-clearance-process-about-get-its-biggest-overhaul-50-years/155229/>.
- Obama, Barack. Executive Order 13526 of December 29, 2009. “Classified National Security Information.” *Code of Federal Regulations*, title 3 (2010): 707–731. <https://www.gpo.gov/fdsys/pkg/FR-2010-01-05/pdf/E9-31418.pdf>.
- Office of Freedom of Information. *Report on DoD Plans to Adopt Continuous Evaluation (CE) and Insider Threat Capabilities*. Washington, DC: Department of Defense, 2015. <https://fas.org/sgp/othergov/dod/ce-2015.pdf>.
- Office of Inspector General. *The DHS Personnel Security Process*. OIG Report No. OIG-09-65. Washington, DC: Department of Homeland Security, 2009. <https://permanent.access.gpo.gov/gpo14559/OIG09-65May09.pdf>.
- Office of the Director of National Intelligence. *IRTPA Title III Annual Report for 2010*. Washington, DC: Office of the Director of National Intelligence, 2011. <https://fas.org/irp/dni/irtpa-2011.pdf>.
- Ogrysko, Nicole. “DoD to Reorganize, Create New Security Clearance Organization.” Federal News Network, November 20, 2018. <https://federalnewsnetwork.com/reorganization/2018/11/dod-to-reorganize-create-new-security-clearance-organization/>.

- Senate Select Committee on Intelligence. *Statement of David J. Berteau, President & CEO, Professional Services Council, before the Senate Select Committee on Intelligence*. Washington, DC: Senate Select Committee on Intelligence, 2018. <https://www.intelligence.senate.gov/sites/default/files/documents/os-dberteau-030718.pdf>.
- . *Statement of Kevin Phillips, CEO ManTech Inc., Hearing on Security Reform*. Washington, DC: Senate Select Committee on Intelligence, 2018. <https://www.intelligence.senate.gov/sites/default/files/documents/os-kphillips-030718.pdf>.
- U.S. Senate. 2845. 115th Cong., 2nd sess. (2017–2018). https://fas.org/irp/congress/2004_rpt/s2845-sum.pdf.
- United States Office of Personnel Management. *FY 2018 Investigations Reimbursable Billing Rates Effective October 1, 2017*. Washington, DC: National Background Investigations Bureau, 2017. <https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/2017/fin-17-04.pdf>.
- . *FY 2019 Investigations Reimbursable Billing Rates Effective October 1, 2018*. Washington, DC: National Background Investigations Bureau, 2017. <https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/2017/fin-17-05.pdf>.
- . *Statement of Charles S. Phalen, Jr., Director, National Background Investigations Bureau, U.S. Office of Personnel Management before the Select Committee on Intelligence United States Senate on “Security Clearance Reform.”* Washington, DC: United States Office of Personnel Management, 2018. <https://www.intelligence.senate.gov/sites/default/files/documents/os-cphalen-030718.pdf>.
- White, Jay D. *Managing Information in the Public Sector*. Armonk, NY: M.E. Sharpe, Inc., 2007. <https://ebookcentral.proquest.com/lib/ebook-nps/detail.action?docID=302467>.
- Whyte, Sally. “The Govt’s Plans to Slash Backlog of Security Clearances.” *Sydney Morning Herald*, June 25, 2018. <https://www.smh.com.au/politics/federal/the-govt-s-plans-to-slash-backlog-of-security-clearances-20180620-p4zmot.html>.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California