NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMMIGRATION ADJUDICATION REFORM: THE CASE FOR AUTOMATION

by

Abigail J. Sanford

September 2014

Thesis Advisor: Robert Bach
Second Reader: Richard Bergin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
IMMIGRATION ADJUDICATION REFORM: THE CASE FOR AUTOMATION

5. FUNDING NUMBERS

6. AUTHOR(S) Abigail J. Sanford

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

A bill that has passed the United States Senate, S. 744, proposes a "Lawful Prospective Immigrant" (LPI) status and a "path to Citizenship" for an estimated 11–12 million undocumented immigrants in the United States. United States Citizenship and Immigration Services (USCIS) is the agency that would be responsible for processing applications for LPI status or other immigration benefits authorized by immigration reform legislation or administrative relief programs introduced by the White House. Current agency receipts of applications for immigration benefits range between 6 and 7 million per year. Depending on the eligibility criteria for new immigration benefits, agency receipts could triple. The operational impact of these legislative or executive actions on USCIS could bear significant national security risks.

This study evaluates whether the implementation of automated tools would mitigate external operational impacts on USCIS. Two existing automated systems are studied. The Secure Flight system, operated by the Transportation Security Administration (TSA), and the Automated Continuous Evaluation System (ACES) as utilized in the Joint Reform Effort (JRE) were selected for their complexity, maturity, and similarity to immigration adjudications. This analysis demonstrates that automated tools can improve the quality of immigration adjudications by supporting a comprehensive assessment, including accuracy, timeliness, completeness and validity. Further, automation would improve the agency's operational responsiveness when external factors such as policy changes affect workloads. These factors thereby improve national security by supporting the agency's mission to uphold the integrity of the immigration system and to prevent and intercept illicit actors from entering or remaining in the United States.

14. SUBJECT TERMS Automated Records Checks, Background Checks, Decision Support Systems, Immigration Adjudications, Immigration Reform, Investigations, National Security, Operational Efficiency, Resource Allocation

15. NUMBER OF PAGES
149

16. PRICE CODE

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

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IMMIGRATION ADJUDICATION REFORM: THE CASE FOR AUTOMATION

Abigail J. Sanford
United States Citizenship and Immigration Services
B.S., The George Washington University, 1998
M.A., The University of Michigan–Ann Arbor, 2000

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
September 2014**

Author: Abigail J. Sanford

Approved by: Robert Bach, Ph.D.
Thesis Advisor

Richard Bergin
Second Reader

Mohammed Hafez, Ph.D.
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

A bill that has passed the United States Senate, S. 744, proposes a "Lawful Prospective Immigrant" (LPI) status and a "path to Citizenship" for an estimated 11–12 million undocumented immigrants in the United States. United States Citizenship and Immigration Services (USCIS) is the agency that would be responsible for processing applications for LPI status or other immigration benefits authorized by immigration reform legislation or administrative relief programs introduced by the White House. Current agency receipts of applications for immigration benefits range between 6 and 7 million per year. Depending on the eligibility criteria for new immigration benefits, agency receipts could triple. The operational impact of these legislative or executive actions on USCIS could bear significant national security risks.

This study evaluates whether the implementation of automated tools would mitigate external operational impacts on USCIS. Two existing automated systems are studied. The Secure Flight system, operated by the Transportation Security Administration (TSA), and the Automated Continuous Evaluation System (ACES) as utilized in the Joint Reform Effort (JRE) were selected for their complexity, maturity, and similarity to immigration adjudications. This analysis demonstrates that automated tools can improve the quality of immigration adjudications by supporting a comprehensive assessment, including accuracy, timeliness, completeness and validity. Further, automation would improve the agency's operational responsiveness when external factors such as policy changes affect workloads. These factors thereby improve national security by supporting the agency's mission to uphold the integrity of the immigration system and to prevent and intercept illicit actors from entering or remaining in the United States.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACES	Automated Continuing Evaluation System
ACLU	American Civil Liberties Union
AFM	Adjudicator's Field Manual
AILA	American Immigration Lawyers Association
ANICI	Access National Agency Check and Inquiries
AR	Administrative Relief
ARC	Automated Records Checks
ARS	automated reservation systems
BI	Background Investigation
BPPR	boarding pass printing result
CBP	Customs and Border Protection
CDC	Center for Disease Control
CE	Continuous Evaluation
CIR	Comprehensive Immigration Reform
COTS	commercial-off-the-shelf
CSA	Customer Service Agent
DACA	Deferred Action for Childhood Arrivals
DBS	database systems
DHS	Department of Homeland Security
DHS CIO	DHS Chief Information Officer
DHS OIG	DHS Office of the Inspector General
DHS TRIP	DHS Travel Redress Inquiry Program
DOD	Department of Defense
DOJ	Department of Justice
DOJ OIG	DOJ Office of the Inspector General
DSS	decision support system
EFF	Electronic Frontier Foundation
EFI	Expandable Focused Investigation
EOD	enter on duty
FBI	Federal Bureau of Investigation

FDNS	Fraud Detection and National Security
FTE	full-time equivalent
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
ICE	Immigration and Customs Enforcement
IO	Immigration Officers
IRTPA	Intelligence Reform and Terrorist Prevention Act of 2004
ISO	Immigration Services Officers
JRE	Joint Reform Effort
KST	known or suspected terrorists
LPI	Lawful Prospective Immigrant
MBI	Moderate Risk Background Investigation
MCDSS	multiple criteria decision support systems
NACI	National Agency Check and Inquiries
NACLC	National Agency Check with Law and Credit
NARA	National Archives and Records Administration
NBTA	Global Business Travel Association
NCIC	National Crime Information Center
NPRM	Notice of Public Rule Making
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPM-FIS	OPM Federal Investigative Services
OSD	Office of the Secretary of Defense
PAC	Performance Accountability Council
PERSEREC	Defense Personnel and Security Research Center
PIA	Privacy Impact Analysis
PII	personally identifiable information
PNR	passenger name records
PPR	Phased Periodic Reinvestigation

PT	Public Trust
QHSR	Quadrennial Homeland Security Review
RBS	risk-based security
RFE	Request for Evidence
SAP	Special Access Programs
SEVIS	Student & Exchange Visitor Information System
SFA	Secure Flight Analyst
SFPD	Secure Flight Passenger Data
SORN	System of Records Notice
SSBI	Single Scope Background Investigation
SSBI-PR	SSBI Periodic Reinvestigation
TIM	Technology Infrastructure Modernization
TPS	Temporary Protected Status
TS	Top Secret
TS/SCI	TS with Sensitive Compartmented Information
TSA	Transportation Security Administration
TSC	Terrorism Screening Center
TSDB	Terrorist Screening Database
TSNM	Transportation Sector Network Management
USCIS	United States Citizenship and Immigration Services

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

External factors affecting immigration adjudication procedures, such as the implementation of Comprehensive Immigration Reform (CIR) or presidentially issued Administrative Relief (AR), will significantly impact operational efficiency at United States Citizenship and Immigration Services (USCIS). Currently, USCIS conducts manual background checks and other records checks of immigration benefit applicants. The estimated impact of CIR or AR on current agency operations is potentially paralyzing. The resulting slow processing times may mean that background investigations on applicants are not conducted in a thorough or timely fashion, thus permitting those who seek to harm the United States easier entry into the country. This will impact our national security.

This thesis examines the potential benefits and costs of utilizing automation tools and decision support systems in the immigration adjudications process. Two existing cases are studied: Transportation Security Administration's (TSA's) Secure Flight and the Department of Defense's (DOD's) Automated Continuous Evaluation System (ACES). These systems became prioritized only *after* major security issues—the attacks of 9/11 and the Navy Yard shooting—highlighted poor operations. Congress mandated improvements to aviation security and the security clearance process through the Intelligence Reform and Terrorism Prevention Act (IRPTA) of 2004, in part to enact several recommendations of the 9/11 Commission Report. The Navy Yard Shooting brought new attention to the effort for Security Clearance Reform.[1] Operational improvements to immigration adjudications processes through the implementation of automation tools must be prioritized *before* a major security incident requires them.

In 2003, changes in immigration adjudications procedures mandated additional background checks and expanded the range of applicants that were required to submit

[1] Jack Moore. Federal News Radio Online. "White House backs 13 recommendations to improve security clearance process." March 19 2014. http://www.federalnewsradio.com/520/3585372/White-House-backs-13-recommendations-to-improve-security-clearance-process .

fingerprints and other biometrics in support of their applications.[2] These operational changes resulted in a peak backlog of 3.85 million cases by January 2004.[3] The agency continued to conduct operations manually, and it reduced the backlog by utilizing overtime resources. A backlog of 3.85 million cases represents a little more than half of the agency's current workload of 6 to 7 million cases per year.

An approximation of the potential workload impact of CIR or AR must take into consideration the compound nature of the process to adjudicate applications. The initial influx of applications could be 11–12 million,[4] however, evidentiary requirements, supplementary applications for employment authorization, reapplications, potential adjustments of status to Lawful Permanent Resident (LPR), and potential Citizenship applications compound the issue of simply tripling receipts of applications. Each of these applications also requires USCIS adjudication resources to process, thus supporting the prediction of a permanent increase in the agency's workload.

Though using overtime resources was successful in 2004 for eliminating a backlog of an additional 50% of the typical workload, it would have little effect on a growing backlog of this magnitude. A permanent increase in staffing levels is not a long-term strategy for optimizing the agency's operations and improving national security. The policy of developing and implementing a decision support tool to automatically check national security systems and other records systems is supported by the findings of this analysis.

The fundamental factors for evaluating the policy decision to implement automation tools for immigration adjudication procedures are:

---

[2] U.S. Department of Homeland Security, United States Citizenship and Immigration Services. *Backlog Elimination Plan: Fiscal Year 2006, 3rd Quarter Update*. (Washington, DC: Department of Homeland Security, December 11, 2006). http://www.uscis.gov/sites/default/files/USCIS/Resources/Reports%20and%20Studies/backlog_FY06Q3.pdf .

[3] U.S. Department of Homeland Security, United States Citizenship and Immigration Services. Backlog Elimination Plan: Fiscal Year 2006, 3rd Quarter Update. (Washington, DC: Department of Homeland Security, December 11, 2006). http://www.uscis.gov/sites/default/files/USCIS/Resources/Reports%20and%20Studies/backlog_FY06Q3.pdf.

[4] Jeffrey S. Passel, D'Vera Cohn, and Ana Gonzalez-Barrera. "Population Decline of Unauthorized Immigrants Stalls, May Have Reversed." Pew Research Hispanic Trends Report. September 23, 2013. http://www.pewhispanic.org/2013/09/23/population-decline-of-unauthorized-immigrants-stalls-may-have-reversed/.

- Expected benefits to stakeholders;
- Potential improvements in operational efficiency, and;
- Potential reduction of risks to national security.

These factors are evaluated as *substantially demonstrated* by both Secure Flight and ACES. These systems each offer a strong and suitable comparison to immigration adjudications. The model suggested by these case studies involves the use of automated rules-based querying of an individual's identifying information on multiple national security systems and a "case-flagging strategy" that sorts cases with adverse or derogatory information for further review. This model appears to optimize the distribution of operational resources, thus improving national security. This model is evaluated as valid for immigration adjudications, and the factors could be *substantially achieved* if the model is implemented at USCIS.

Recommendations:

1) USCIS should develop automation tools for immigration adjudications regardless of the status of immigration reform or other immigration policy changes.

Changes in agency workload can be affected by many external factors, including the addition of new benefit types per new law or executive order; international crises (war, political unrest, natural disasters, or other) that affect immigration patterns; seasonal or cyclical increases in application receipts; and many others. This analysis shows that automated tools to support adjudication and investigative procedures can improve operational responsiveness to such factors. The agency could realize benefits for operational efficiency and national security by implementing automation tools even in the absence of immigration reform.

2) If the Congress or the President makes changes to immigration policy, funding specifically to support the development of automation tools at USCIS should be allocated.

Given the cost and challenge of developing an automation tool, resource constraints at USCIS will limit progress towards its implementation. Current efforts to

develop an electronic application, a case management system, and the adjudications platform called “USCIS ELIS” under the Transformation Program are significantly behind original plans, both in schedule and budget. While automated records checks could reasonably fit into the development of USCIS ELIS, the funding and resources to build it properly would be evaluated for priority among all other agency information technology efforts.

Operational inefficiencies or customer service problems that are likely to arise due to the expected workload impact of CIR or AR could provide the agency with leverage for additional funding to develop and implement an automation tool. However, such an operational efficiency gap would pose a significant national security risk. Therefore, Congress or the White House should fund the development of an automation tool for immigration adjudications *in conjunction* with significant changes to immigration policy or procedure.

ACKNOWLEDGMENTS

It was indeed a privilege and deep honor to accept the invitation to participate in the master's program at the Center for Homeland Defense and Security (CHDS). While I knew writing a thesis was a required element of the program, I blocked it out of my mind when I accepted the opportunity to join Cohort 1301. Thankfully, the program is designed to guide students along the thesis journey from early on, so I was quickly forced to give thought to "what do I care about enough to research, write about, and live with for over a year?" My idea was born relatively quickly, and I am grateful for the input from my colloquium advisor, Dr. Nadav Morag, as well as all instructors in the program. Thank you.

I am further indebted to my thesis advisor and reader, Dr. Robert Bach and Mr. Richard Bergin. You pushed me to refine my way of thinking, to dig deeper, and to "forge ahead!" Thank you. For pointing me in the right direction with my research, I'd like to specifically thank Mr. Kevin Greeley with United States Citizenship and Immigration Services (USCIS), Mr. Kenneth Fletcher with the Transportation Security Administration (TSA), and Ms. Leissa Nelson with the Defense Personnel and Security Research Center (PERSEREC).

The 18-month program at CHDS has been the most challenging academic endeavor of my life. It was nothing and everything I thought it would be, and then some. The camaraderie of my class, Cohorts 1301/1302, made it even more gratifying. The respect and kinship developed during those weeks on the third floor of Watkins Hall have been forged in iron. I thank you for refining my thoughts.

The support, guidance, and love from my family and friends throughout this program have been unfailing. Without question, the woman who served as my editor deserves the most acknowledgement for this thesis. As it turns out, my mother, Cheryl Sanford, was an English teacher in the early part of her education career. I have never known anyone who could remember all the rules of the comma the way that she can. More than just the wielder of the red pen, though, she served as my audience, my friend,

my sounding board, my cheerleader, and at times my therapist throughout this process. Without her strength as a human being and unconditional love for a daughter who occasionally got frustrated with her, my journey would have been a bit more difficult.

This one is for you, Mom.

I. BACKGROUND

A. PROBLEM STATEMENT

United States Citizenship and Immigration Services (USCIS, or "the Agency") processes between 6 and 7 million applications or petitions for immigration benefit requests each year. These include requests for visitor or student visas, temporary work permits, family-based petitions such as legal permanent residency for foreign spouses, and citizenship requests, among others. Depending on the type of request, each petition or application requires an adjudication or decision based on a review of information related to the applicant or petitioner. Information on the applicant or petitioner or his/her dependents is either provided on the request form or collected by the USCIS adjudicator from government or other sources. Criteria for granting immigration benefit requests are based in policies from the Agency and other governing bodies, including statutes and regulations such as the Immigration and Nationality Act (1952) and Title 8 of the Code of Federal Regulations (commonly referred to as "8 CFR"), field and administrative manuals, handbooks and operations instructions, published precedent decisions, and memoranda and cables specifically designated as policy. Occasionally, official correspondences from USCIS headquarters or Members of Congress may affect adjudications. The Agency spends significant resources to process immigration benefit requests. In addition to Agency operational resources, immigration benefit requests require the time of trained adjudicators, background check officers, fraud officers, verification officers, records clerks, and others to process.

Decades ago, information necessary to adjudicate immigration benefit requests was stored throughout several government agencies in paper files. More recently, electronic systems to improve the storage and retrieval of information were developed and deployed throughout USCIS and other agencies. These systems can generally be categorized as "database systems" (DBSs). DBSs also enabled the creation, storage, and usage of new data in the adjudications process. Use of this additional data may lead to

improved adjudications.[1] However, this explosion of data and the associated DBSs have required adjudicators to retrieve information from multiple database systems in order to conduct thorough investigations. As a result, processing immigration benefit requests requires general familiarity with several DBSs, including their contents and structure, the query language for each system, their location on a network, access to that network if a database resides outside USCIS, and more. Each adjudicator must break down each investigation into a series of retrieval tasks, conduct queries of several sources, and then temporarily store, transfer, or synthesize intermediate results. Furthermore, the DBS landscape is continually changing. As systems are upgraded, replaced, or retired, adjudicators must continuously learn new systems, new query languages, new contents structures, and the interpretation of new results.

Compounding the problems associated with querying multiple DBSs are external factors that may affect Agency workload or procedures. For example, the Agency redesigned the N-400 "Application for Naturalization." Prior to its public release, there was a spike in receipts of applications on the existing form, resulting in a temporary increase in workload. As another example, Agency procedures were impacted by changes in laws and regulations due to the heightened national security environment after the terror attacks of September 11, 2001. Changes in adjudications procedures in 2003 mandated additional background checks and expanded the range of applicants that were required to submit fingerprints and other biometrics in support of their applications.[2] These operational changes resulted in a peak backlog of 3.85 million cases in January 2004.[3]

The United States Congress is currently evaluating Comprehensive Immigration Reform (CIR) legislation. If CIR passes, it would significantly affect both Agency workload and procedures. A bill that has already passed the United States Senate, S.

[1] Andrew McAfee and Erik Brynjolfsson. "Big Data: The Management Revolution." Harvard Business Review, 90, no. 10 (October 2012): 60–68.

[2] U.S. Department of Homeland Security, United States Citizenship and Immigration Services, "Backlog Elimination Plan." Fiscal Year 2006, 3rd Quarter Update. (Washington, DC: Department of Homeland Security, December 11, 2006). http://www.uscis.gov/sites/default/files/USCIS/Resources/Reports%20and%20Studies/backlog_FY06Q3.pdf.

[3] Ibid.

744,[4] proposes a "Lawful Prospective Immigrant" (LPI) status that would provide a "path to Citizenship" for an estimated 11–12 million undocumented immigrants[5] in the United States. As with other immigration benefits, applications for LPI or any other status created by CIR would be processed by USCIS. Agency leaders estimate that the current workload of 6 to 7 million applications per year would immediately triple in the year following the implementation of CIR.[6] Additionally, they estimate that steady-state workload would be about double the current level due to reapplications, adjustments of status, and eventual naturalization applications for the newly eligible LPI population. When CIR becomes a reality, an overwhelming caseload will compound the challenge that USCIS adjudicators and other employees currently face in evaluating immigration benefits requests by querying a significant number of databases to answer questions related to an application.

Figure 1 demonstrates the general procedures for processing an immigration benefit request.

[4] Border Security, Economic Opportunity, and Immigration Modernization Act, S.744, 113th Cong., 1st sess. (2013). http://www.gpo.gov/fdsys/pkg/BILLS-113s744es/pdf/BILLS-113s744es.pdf .

[5] Jeffrey S. Passel, D'Vera Cohn, and Ana Gonzalez-Barrera. "Population Decline of Unauthorized Immigrants Stalls, May Have Reversed." *Pew Research Hispanic Trends Report*. September 23, 2013. http://www.pewhispanic.org/2013/09/23/population-decline-of-unauthorized-immigrants-stalls-may-have-reversed/.

[6] An approximation of the workload impact of S.744 must take into consideration the compound nature of the process that would be created to support Lawful Prospective Immigrant (LPI) status, involving initial applications for status and work authorization, as well as status reapplications and citizenship applications as outlined in the Bill. The initial influx of applications could be 11–12 million; however, the evidentiary requirements of LPI status and the supplementary application for employment authorization compound the issue of simply tripling receipts. Furthermore, the Bill requires reapplication after 6 years, thus increasing the workload baseline. LPIs become eligible to apply for citizenship after 10 years, and naturalized U.S. Citizens become eligible to petition for family members to immigrate or adjust status to lawful permanent residents. Each of these procedures requires USCIS adjudication resources, thus supporting the prediction of a permanent increase in the Agency's workload.

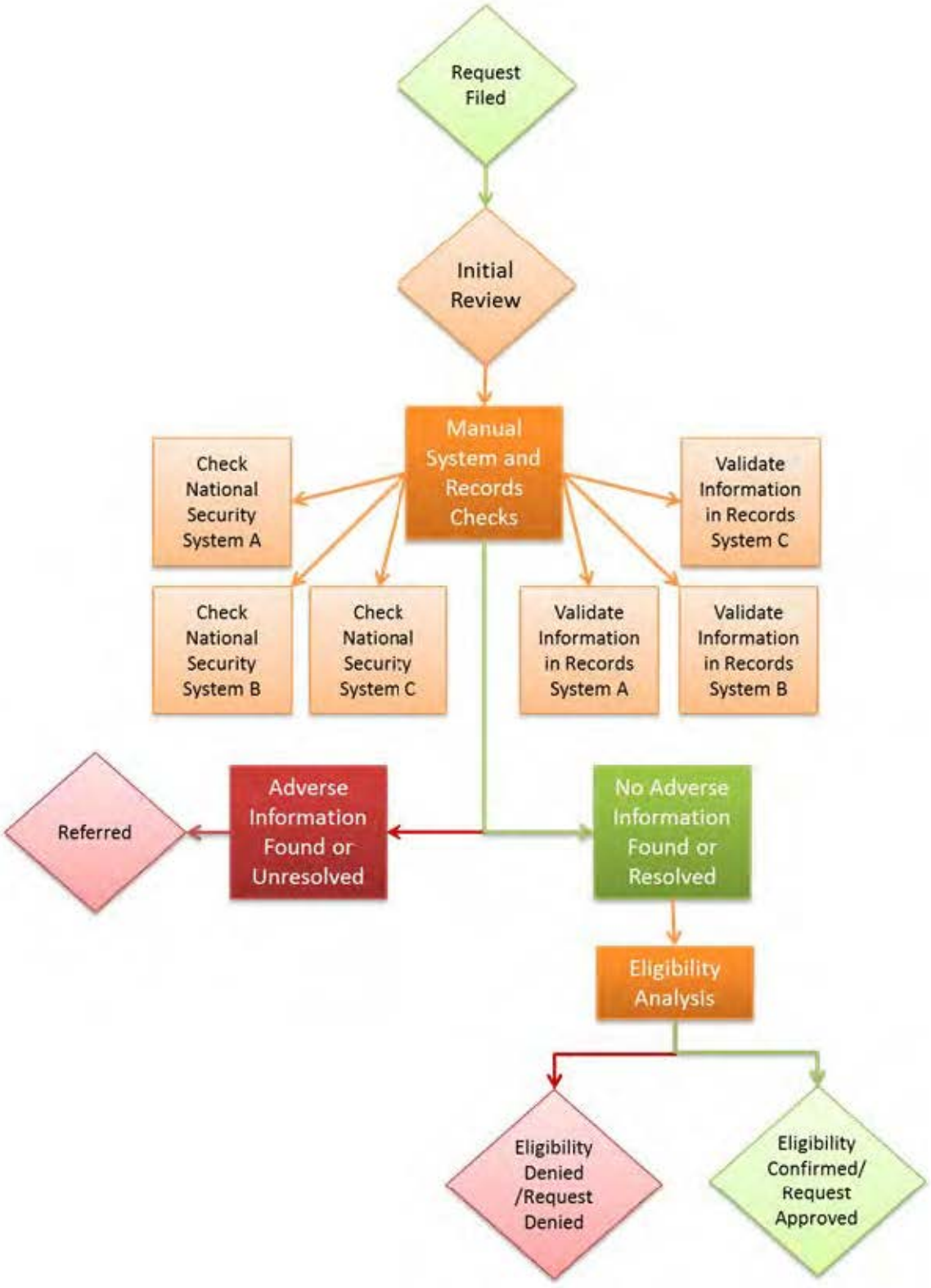

Figure 1. Immigration Benefit Request Processing Overview

A technological tool to automate certain database queries might address some of the operational impact of CIR. In the absence of CIR, such a tool might simply improve existing processing times for immigration adjudications and reduce risks to national security in the current environment and in response to external factors. Categorized as "decision support systems," (DSS) tools to aid in immigration adjudications could be described as the integration of authoritative DBSs coupled with algorithms that perform automated queries and evaluate query results. Depending on the type of benefit request being adjudicated, an automated querying tool could provide varying levels of decision support. For complicated applications, such as the N-400 "Application for Naturalization," which require an interview in addition to background and system checks, a DSS tool might query systems for information on the applicant and then present results to an immigration officer for review with adverse information flagged or otherwise highlighted. For less complex adjudications, such as the I-539 "Application To Extend/ Change Nonimmigrant Status," or extensions of Temporary Protected Status (TPS) for certain asylees, an automated DSS might be able to fully qualify complete applications with little or no adverse information. That is, a DSS could query DBSs using rules based on current policy and regulations, evaluate the results, and significantly reduce the human resources required for adjudications. The system could also identify applications with significant adverse information, focusing in-depth human review on high-risk or complex cases.

USCIS is challenged with balancing the tasks of appropriately adjudicating immigration benefit requests and welcoming lawful immigrants with enhancing national security by limiting fraud and preventing the admission of those who intend harm. As identified in Mission 3 of the Quadrennial Homeland Security Review (QHSR),[7] USCIS plays a key role in reaching the goals of effectively and efficiently administering immigration laws; providing prompt and accurate adjudications; preventing fraud, abuse, and exploitation; eliminating systemic vulnerabilities; and preventing the entry of criminals or dangerous foreign nationals. Meeting these challenges requires operational

[7] U.S. Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland (QHSR)*. (Washington, DC: Department of Homeland Security, February 2010). http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf .

efficiency. However, both the current multi-system procedures and the potential impact of CIR threaten the Agency's capacity to operate effectively and meet these goals. Technology-based decision support tools such as automated querying could improve the Agency's capacity to meet these goals.

B. LITERATURE REVIEW

The main field of research that this study builds upon is Decision Support Systems (DSS). The literature on DSS is mature and vast. Shim et al. provide a review of over three decades of DSS research beginning with its evolution in the 1960s and 1970s from two areas—theoretical studies of organizational decision-making and technical applications and designs.[8] As pointed out by Shim et al., the original concept of DSS that was based on early research by Anthony,[9] Gorry and Morton,[10] and Simon[11] describes types of problems, management activities, and decisions. Simon describes a model spectrum of decision problems from "programmed" to "nonprogrammed," while Gorry and Morton use the terms "structured," "unstructured," and "semi-structured" for their model. Their research supports the development of DSS to deal with the structured portions of a problem with remaining "unstructured" parts reserved for a human decision-maker.

This area of literature is relevant to the investigation of integrating technology and DSS into the processing and adjudication of applications for LPI status. In this decision process, many of the business rules are well known, regulated, and understood. The decision of granting status would conceivably fall towards the "programmed" or "structured" end of the spectrum. This literature also supports the idea of a problem-solving system that involves a hybrid of technology and human decision-making.

---

[8] J. P. Shim, Merrill Warkentin, James F. Courtney, Daniel J. Power, Ramesh Sharda, and Christer Carlsson. "Past, Present, and Future of Decision Support Technology." *Decision Support Systems* 33, no. 2 (2002): 111–126.

[9] R.N. Anthony, *Planning and Control Systems: A Framework for Analysis*. (Cambridge, MA: Harvard University Graduate School of Business Administration, 1965).

[10] George A. Gorry and Michael S. Morton. "A Framework for Management Information Systems." *Sloan Management Review* 13, no. 1 (1971): 50–70.

[11] Herbert A. Simon. "The New Science of Management Decision," in *The Ford Distinguished Lectures*, Volume 3. (New York, NY: Harper & Brothers, 1960).

Jelassi, Jarke, and Stohr (1985) provide a very basic summary of the advantages of multiple criteria decision support systems (MCDSS), such as their ability to support the analysis of multiple criteria at once in an interactive way. MCDSS is the branch of decision support that is the most relevant to immigration adjudications since there are several system checks that an applicant would have to pass to qualify for benefits. Jelassi et al. suggest that reasonable models can be developed to appropriately address semi-structured problems (like immigration benefit requests) with such a system.[12] Beyond laying out the criteria for a system, they do not provide any further argument as to why this kind of system is beneficial. The question of the appropriateness of DSS in a homeland security environment requires further investigation.

What appears to be largely missing from the academic literature is an evaluation of automated intelligent querying of heterogeneous datasets in the homeland security enterprise. Ceruti, Wilcox, and Powers (2004) purport that to maximize the utility of knowledge management systems, "the knowledge in the system must be abstracted, structured, and otherwise clustered in a suitable manner that facilitates its understanding, verification, validation, maintenance, management, testing and interoperability."[13] They offer types of data analysis techniques such as clustering or partitioning that could be performed on knowledge management systems in the context of military command and control. They touch on the subject of integrated systems, suggesting that participants in a system must develop policies for supplying and extracting data.[14]

A significant amount of technical and analytical literature exists in areas of research related to the tools being evaluated in this thesis. The literature on decision support systems is at least 30 years deep. However, applications related to homeland or national security do not appear frequently or in-depth in academic literature. Research to evaluate automated background checking or other government information sharing

---

[12] Mohamed Tawfik Jelassi, Matthias Jarke and Edward A. Stohr. "Designing a Generalized Multiple-Criteria Decision Support System." *Journal of Management Information Systems* 1 (Spring 1985):4.

[13] M.G. Ceruti, D.R. Wilcox, and B. Powers. Space and Naval Warfare Systems Center, San Diego, CA. "Knowledge Management for Command and Control." Paper for the 2004 Command and Control Research and Technology Symposium, June 15–17, 2004.

[14] Ibid.

activities is not fully explored. The use of decision support tools for homeland or national security requires further investigation and analysis.

Several documents related to the government programs analyzed in the case studies of this thesis were analyzed. These include reports from the Government Accountability Office (GAO); the Department of Homeland Security (DHS) Office of the Inspector General (DHS OIG); DHS component offices, including the Transportation Security Administration (TSA) and United States Citizenship and Immigration Services (USCIS); the Department of Justice (DOJ) Office of the Inspector General; reports from the White House; official testimonies before the Congress; presentations made by government officials at conferences; public government websites; reports from the news media; and various other public reports. These are cited as appropriate.

C. RESEARCH DESIGN AND METHODOLOGY

The central question of this thesis is whether national security could be improved by using decision support systems in immigration adjudications. This thesis will attempt to evaluate whether DSS in the form of automated queries would improve the quality of adjudications by supporting a comprehensive assessment, including accuracy, timeliness, completeness and validity. This thesis will also attempt to evaluate whether automation would improve the Agency's operational responsiveness when external factors such as policy changes affect workloads. If demonstrated, these factors would improve national security by supporting the Agency's mission to uphold the integrity of the immigration system and prevent and intercept illicit actors from entering or remaining in the United States.

Throughout this thesis, "automation" and DSS refer to the automatic querying of existing data sources to support immigration adjudications. As previously noted, the adjudication of benefit requests vary in their level of complexity. As a result, complete automation of adjudication procedures would apply to few immigration benefit request types.

Several government agencies in the United States and abroad utilize decision support systems to automate certain adjudicative procedures. Because actual testing of

automation and DSS for immigration adjudications would require its development and implementation, the proposal of utilizing such systems cannot be studied directly. This thesis will examine two existing decision support systems as proxies for analysis. The decision support systems in this analysis were selected for their complexity, maturity, and similarity to immigration adjudications.

The following two cases will be analyzed:

Secure Flight (Transportation Security Administration)

The Transportation Security Administration (TSA) utilizes its "Secure Flight" program to adjudicate a passenger's ability to fly on a commercial airline. It uses automated business rules and searches of databases and watch lists.[15] In addition, TSA passenger screening program, called "Pre✔" ("pre-check"), utilizes risk data from Secure Flight to sort passengers for expedited or enhanced screening.

Automated Continuing Evaluation System (ACES) (Department of Defense)

ACES is an automated pilot project that can query over 40 different government and commercial database records to evaluate the behavior of previously cleared personnel during reinvestigation.[16]

As is discussed in detail in Chapter IV of this analysis, there are significant reasons why each of these systems offers a strong and suitable comparison to immigration adjudications. First, the general procedures are similar. Each of the cases, as well as immigration adjudications, follows a general process of *application*, *investigation*, *adjudication*, and *post-decision activity*. Second, automation and decision support tools are used to support the same step in the overall process: *investigation*. Third, each of the two case systems utilizes rules-based querying of an individual's identifying information on multiple national security systems. Finally, a "case-flagging strategy" is used in each of the cases that appears to optimize the distribution of

[15] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Program." http://www.tsa.gov/stakeholders/secureflight-program. (Accessed January 21, 2014).

[16] Defense Personnel Security Research Center (PERSEREC). "Current Initiatives." http://www.dhra.mil/perserec/currentinitiatives.html. (Accessed June 24, 2014).

operational resources. This model, if valid, would be appropriate to utilize for immigration adjudications to improve operational efficiency, thus improving national security.

For each of the cases studied, the benefits and costs of automation and DSS will be analyzed with respect to stakeholders, Agency or other government operations, and national security objectives. The cases will be examined in Chapters II and III.

Each of the case studies will examine the following:

- What are the benefits and costs of automation to important program stakeholders?
- What operational efficiencies do the respective agencies gain from automation in each case study? What implementation costs are required for each system?
- What reductions or increases in risk to national security are attributable to the implementation of automation and decision support systems in each case study?

Chapter IV will relate the findings of costs and benefits in the case studies to the immigration adjudications process. Drawing on the similarities of the processes and recommended use of automation for immigration adjudications, the following questions will be addressed:

- What benefits, costs, and operational efficiencies could be realized if automation was utilized in immigration benefits adjudication?
- Would risks to national security decrease or increase by automating immigration adjudications?

These elements are fundamental factors that must be considered when evaluating the policy decision to implement automation tools for immigration adjudication procedures. As will be shown in each of the cases, the resources required to implement automation and decision support tools are significant. Hundreds of millions of dollars have been invested in each of the cases, and a similar investment would be required for immigration adjudications. Substantial benefits to stakeholders, improvements to operational efficiency, and the reduction of risks to national security would justify the

expenditure of resources to develop automation tools. If these can be shown, they would support the policy of implementing automation tools for immigration adjudications.

When available, dollar value estimates or actual development costs for decision support tools will be provided. However, the dollar value of many of the benefits and costs of automation in the examined cases is difficult to quantify and will be difficult to ascribe to the costs and benefits associated with DSS/automation for immigration adjudications.

Quantifying the value of national security benefits is particularly challenging because estimating the cost of *events prevented* requires an understanding of risks that may only be available to the intelligence community. The scope of this analysis will not include a dollar value for these types of benefits.

Despite these challenges in ascribing dollar values to costs and benefits, this analysis remains constructive for evaluating the policy decision of implementing automation tools for immigration adjudication procedures. Government activity is unlike certain endeavors in private industry where “return on investment” must be shown, or where profit must be made or shareholder value increased in order to sustain that endeavor. Government activity may not always involve a full cost-benefit analysis prior to implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

II. SECURE FLIGHT CASE STUDY

A. PROGRAM OVERVIEW

Secure Flight is the Transportation Security Administration's (TSA) program for aviation security whereby passenger information is matched against information of individuals with known or suspected links to terrorism. The purpose of matching passenger information is to improve aviation and national security by preventing suspected or known terrorists from boarding aircraft either bound for or operating within the United States. The volume of air travel to or within the United States requires that Secure Flight prescreens an average of 2 million passengers every day.[17] Because of this volume, automation of the matching and alerting process is essential for the program's success.

B. PROGRAM BACKGROUND

In July 2004, the National Commission on Terrorist Attacks Upon the United States ("the 9/11 Commission") recommended improvements to national security. Key recommendations for aviation security were to improve the system of matching passenger information to terror watch lists and to use expanded lists for match confirmation when needed.[18]

The 9/11 Commission recommended that watch list matching be performed by the federal government rather than by aircraft operators. Under the authority of 49 U.S.C. section 114 of the Intelligence Reform and Terrorism Prevention Act (IRTPA),[19] passed by Congress in 2004, this recommendation became a law that requires the Department of Homeland Security (DHS) to perform this national security function. Between 2004 and

[17] U.S. Department of Homeland Security, Office of Inspector General. *Implementation and Coordination of TSA's Secure Flight Program (redacted version).* (OIG-12-94)(Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

[18] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report.* (New York: W.W. Norton & Co., 2004).

[19] Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA). Pub. L. No. 108–458, 118 Stat. 3638 (Dec. 17, 2004), codified at 42 U.S.C. §2000ee, 50 U.S.C. §403-1 et seq., §403-3 et seq., §404o et. seq.

2008, the Transportation Security Administration (TSA) developed, tested, and implemented a program called "Secure Flight" to meet this mandate. The Secure Flight Final Rule, issued October 28, 2008, provided the regulatory authority for the full implementation of the Secure Flight program.[20] As of November 2010, TSA has fully assumed the function of watch-list matching from private air carriers.[21]

Secure Flight now conducts automated prescreening of airline passengers for all covered U.S. and foreign flights into, out of, and within the United States, including point-to-point international flights operated by U.S. airlines and flights that overfly, but do not land in, the continental United States.[22] The Secure Flight automated system uses pre-programmed query logic[23] to match passenger names against the No Fly and Selectee lists.[24] According to Secure Flight program procedures, an individual who is matched to the No Fly List is to be prevented from boarding an aircraft, and an individual who is matched to the Selectee List is to be inspected with enhanced screening procedures.[25]

1. The No Fly and Selectee Lists

The No Fly and Selectee lists are subsets of the Terrorist Screening Database (TSDB) that is maintained by the Terrorist Screening Center (TSC).[26] The Department of Justice's (DOJ) Federal Bureau of Investigation (FBI) established the Terrorist Screening Center (TSC)[27] pursuant to Homeland Security Presidential Directive–6 (HSPD–6), published in September 2003. HSPD–6 mandated that the "Attorney General shall

---

[20] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Overview." March 19, 2014. http://www.tsa.gov/stakeholders/secure-flight-program.

[21] Ibid.

[22] Ibid.

[23] *Code of Federal Regulations*, Privacy Act of 1974: Implementation of Exemptions; Secure Flight Records, title 49, sec. 1507. http://www.dhs.gov/xlibrary/assets/privacy/privacy_nprm_tsa_secureflight.pdf.

[24] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Overview." March 19, 2014. http://www.tsa.gov/stakeholders/secure-flight-program.

[25] Ibid.

[26] U.S Government Accountability Office. *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks*. (GAO-09-292) (Washington, DC: GPO, 2009). http://www.gao.gov/products/GAO-09-292.

[27] Ibid.

establish an organization to consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information processes."[28]

Homeland Security Presidential Directive–11, issued in August 2004, clarified the intended contents of the TSDB as information about "individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism."[29] Such individuals are commonly referred to as "known or reasonably suspected terrorists" (KST).

The inclusion criteria for the No Fly and Selectee lists are sensitive or classified and not available in public documents. A redacted report from the Department of Homeland Security Office of the Inspector General (DHS OIG) in 2009 indicates "the requirements are considerably more stringent than the TSDB's known or reasonably suspected standard."[30] The process for nomination of individuals to the TSDB is itself complex and scrutinized.[31] The "stringent" requirements for the inclusion of an individual on the No Fly or Selectee lists may be due to public concern for privacy or misidentification.

2. Program Mission

> The mission of the Secure Flight program is to strengthen the security of commercial air travel into, out of, within, and over the United States through the use of improved and expanded watch list matching using risk-based security measures.
>
> –Secure Flight Overview, Transportation Security Administration.[32]

---

[28] White House. *Homeland Security Presidential Directive–6: Integration and Use of Screening Information to Protect Against Terrorism*. (September 16, 2003).

[29] White House. *Homeland Security Presidential Directive–11: Comprehensive Terrorist-Related Screening Procedures*. (August 27, 2004).

[30] U.S. Department of Homeland Security, Office of Inspector General. *Role of the No Fly and Selectee Lists in Securing Commercial Aviation (redacted version).* OIG-09-64, (Washington, DC: Department of Homeland Security, July 2009). http://www.oig.dhs.gov/assets/Mgmt/OIGr_09-64_Jul09.pdf.

[31] Ibid.

[32] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Overview." March 19, 2014. http://www.tsa.gov/stakeholders/secure-flight-program.

The recommendation by the 9/11 Commission that the federal government assumes responsibility for watch list matching and the subsequent legislation provided by the IRTPA was intended to improve aviation security. Prior to the implementation of Secure Flight, individual airlines conducted watch list matching using a watch list provided by TSA and their own matching processes.[33] Static versions of watch lists were distributed,[34] and the airlines were entrusted with the task of screening passenger information and inhibiting matched passengers from boarding aircraft. Because each aircraft operator conducted its own processes, matching results, threat assessments, and the coordination of law enforcement responses were not consistent across the aviation industry.[35] By assuming watch list matching responsibilities from private airlines, TSA was tasked with meeting several goals for improved efficacy and security related to aviation security. These include:

1. Eliminating inconsistencies in the passenger watch list matching procedures conducted by air carriers and authorizing the use of a larger set of watch-list records when necessary;

2. Providing earlier identification of potential matches, allowing for expedited notification to law enforcement for coordinated efforts;

3. Providing a fair, equitable, and consistent matching process across all airlines;

4. Reducing the risk of unauthorized disclosure of sensitive watch-list information or compromised watch list data by limiting its distribution;

5. Protecting passengers' personal information from unauthorized use and disclosure by adhering to Privacy Act regulations; and

---

[33] U.S. Department of Homeland Security. *Advance Passenger Information System Pre-Departure Final Rule & Secure Flight Notice of Rule Making.* (Washington, DC: Department of Homeland Security, n.d.). http://www.hlswatch.com/sitedocs/apis-secure-flight-joint-faqs.pdf.

[34] Ibid.

[35] U.S. Department of Homeland Security, Transportation Security Administration, Office of Acquisition. "Official Solicitation for the TSA Secure Flight Resolution Center, call center support." Solicitation No. HSTS02-08-R-TTC159. July 3, 2008. https://www.fbo.gov/index?tab=documents&tabmode=form&subtab=core&tabid=ed9d723a863da7938300737ab3358e07.

6. Reducing the number of individuals who are improperly identified as being on the No Fly or Selectee list through consistent logic and the integration of information from Department of Homeland Security's Travel Redress Inquiry Program (DHS TRIP) so that individuals are less likely to be improperly delayed or prohibited from boarding an aircraft.[36]

C. USE OF DECISION SUPPORT SYSTEMS

Under the Secure Flight program, passengers are required to provide Secure Flight Passenger Data (SFPD) including their full name (as it appears on the government-issued identification they plan to use when traveling), date of birth, gender and their redress number (if applicable) to the airline when making a reservation.[37] The airline submits SFPD to Secure Flight which vets it through an automated matching system. This automated system is a collection of hardware and Commercial-off-the-Shelf (COTS) software designed to support the requirements of the Secure Flight program.[38] The Secure Flight system matches SFPD against government watch lists including the No Fly, Selectee, and Expanded Selectee Lists; Customs and Border Protection's (CBP) Automated Targeting System—Passenger List; the Center for Disease Control and Prevention Do Not Board Lists; as well as the DHS TRIP Cleared List and Trusted Traveler Programs, such as Global Entry, SENTRI and NEXUS.[39] Secure Flight integrates these DHS redress results into the watch list matching process to help prevent delays of misidentified passengers.[40]

---

[36] U.S. Government Accountability Office. *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks.* (GAO-09–292) (Washington, DC: GPO, 2009). http://www.gao.gov/products/GAO-09-292.

[37] U.S. Department of Homeland Security, Transportation Security Administration. "Frequently Asked Questions—Secure Flight." March 19, 2014. http://www.tsa.gov/content/frequently-asked-questions-secure-flight. (Accessed June 1, 2014).

[38] U.S. Department of Homeland Security, Transportation Security Administration, Office of Acquisition. "Official Solicitation for the TSA Secure Flight Resolution Center, call center support." Solicitation No. HSTS02-08-R-TTC159. July 3, 2008. https://www.fbo.gov/index?tab=documents&tabmode=form&subtab=core&tabid=ed9d723a863da7938300737ab3358e07.

[39] United Airlines. "Secure Flight." http://www.united.com/web/en-US/content/travel/airport/id/secure.aspx. (Accessed May 21, 2014).

[40] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=17. (Accessed May 26, 2014).

For national security purposes, the exact matching logic and querying tools used by Secure Flight are not available in public documents. Publishing the details of watch list matching measures as well as capabilities and vulnerabilities of the watch list matching process could enable targeted individuals to evade detection and thereby impede efforts to ensure transportation security.[41]

However, from a variety of sources including multiple Government Accountability Office reports,[42] an economic impact analysis[43] of the Secure Flight Final Rule, and a report from the DHS Office of the Inspector General,[44] it is known that TSA conducted significant testing of a variety of name-matching technologies to determine the best tools, query logic, and passenger information requirements for the operational Secure Flight Program. The testing was conducted using historical passenger name record data from 27 airlines and a copy of the TSDB.[45] It can also be determined from these reports that TSA tested a variety of name-matching tools and a variety of combinations of passenger data from the samples provided by commercial airlines.[46] The operational testing goals compared the efficacy of Secure Flight's automated watch list matching

---

[41] U.S. Department of Homeland Security, Transportation Security Administration. *Privacy Act of 1974: Implementation of Exemptions; Secure Flight Records.* 49 CFR Part 1507. http://www.dhs.gov/xlibrary/assets/privacy/privacy_nprm_tsa_secureflight.pdf.

[42] U.S. Government Accountability Office. *Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program.* (GAO-06-864T) (Washington, DC: GPO, 2006). http://www.gao.gov/products/GAO-06-864T.

[43] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management. *Regulatory and Economic Analysis. Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

[44] U.S. Department of Homeland Security, Office of Inspector General. *Implementation and Coordination of TSA's Secure Flight Program (redacted version*), (OIG-12-94) (Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

[45] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management. *Regulatory and Economic Analysis. Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

[46] U.S. Department of Homeland Security, Office of Inspector General. *Implementation and Coordination of TSA's Secure Flight Program (redacted version*), (OIG-12-94) (Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

rates with benchmarks set by aircraft operators[47] and included minimizing false positive matches and assuring that matches were made within error thresholds.[48] Furthermore, TSA conducted tests to determine the least and best amount of information to collect from passengers in order to minimize false negatives. That is, these tests determined the least amount of information necessary to collect to achieve efficacy benchmarks. These benchmarks are sensitive or classified and not available in public documents. TSA tested and compared sample sets of passenger name records (PNR) from multiple airlines. These samples revealed that there was considerable diversity in the information that was collected and in the way airlines and travel agents were storing it. These tests helped TSA determine a standardized format for collecting passenger names to ensure consistent and accurate watch list matching across all airlines.[49]

TSA determined that standardizing PNR data collected from passengers to include their date of birth and gender would greatly improve the performance of the name-matching technology by reducing false positives, that is, the number of passengers misidentified as a match to the watch list.[50] At the end of the testing, TSA determined that a passenger's full name, date of birth, and gender are "the minimum amount of personal information necessary to conduct effective watch list matching."[51] Collections of these elements for all passengers on covered flights was federally mandated in the

---

[47] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management, Regulatory and Economic Analysis. *Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

[48] U.S. Government Accountability Office. *Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program*. (GAO-06-864T) (Washington, DC: GPO, 2006). http://www.gao.gov/products/GAO-06-864T.

[49] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management, Regulatory and Economic Analysis. *Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

[50] NBS News.com. "How Secure Flight Works." http://www.nbcnews.com/id/39892975/ns/travel-travel_tips/t/how-secure-flight-works/. (Accessed June 1, 2014).

[51] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Communications Toolkit: Talking Points for Editorial from TSA." July 20, 2010, Version 3.0 http://www.tsa.gov/content/communications-toolkit. (Accessed June 1, 2014).

Secure Flight Final Rule set forth in the Code of Federal Regulations under Title 49, parts 1540 and 1560, and published in the Federal Register Volume 73, Number 209.[52]

The supporting procedures for data submission, match verification, and coordination of efforts are available in public documents. The following is a summary of those procedures.

Aircraft operators must submit SFPD electronically to Secure Flight. Most major air carriers with automated reservation systems (ARS) connect to and transmit passenger data through a DHS portal.[53] For aircraft operators with manual reservation systems, Secure Flight has a web application called "eSecure Flight." Because manual data entry is required to use this system, most major airlines use the direct DHS portal. Many smaller air carriers use eSecure Flight.[54]

An aircraft operator cannot print a passenger's boarding pass until it receives a cleared "boarding pass printing result" (BPPR) from Secure Flight. Secure Flight's automated watch list matching program is responsible for pre-screening an average 2 million passengers every day. The vast majority of SFPD information is automatically cleared by the system, with an average response time of 8.67 seconds for low-priority records and 2.01 seconds for high-priority records.[55] For cleared passengers whose information does not match watch lists, Secure Flight transmits this information to airlines so they may issue boarding passes.[56]

The Secure Flight program has also standardized the procedures for validating and coordinating a response in the event of a watch list match. The procedures require manual review and validation to minimize false positives and to ensure that legitimate

---

[52] *Code of Federal Regulations*, Secure Flight Program; Final Rule, title 49, sec. 154. October 28, 2008. http://www.gpo.gov/fdsys/pkg/FR-2008-10-28/html/E8-25432.htm.

[53] U.S. Department of Homeland Security, Office of Inspector General. *Implementation and Coordination of TSA's Secure Flight Program (redacted version*). (OIG-12-94) (Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

[54] Ibid.

[55] Ibid.

[56] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Overview." March 19, 2014. http://www.tsa.gov/stakeholders/secure-flight-program .

members of the traveling public are distinguished from known or suspected terrorists (KST).[57] If a potential match is made by the Secure Flight automated system, the aircraft operator will receive a negative BPPR and be prevented from printing a boarding pass. The aircraft operator must then contact one of two Secure Flight Resolution Centers (SFRC) to reach a resolution. A Secure Flight Analyst (SFA) then attempts to validate or invalidate the match based on a review of additional information.

The SFA retrieves potential matches from a secure system and manually searches the systems checked by Secure Flight as well as other "intelligence resources."[58] These resources can provide additional details to the SFA who attempts to verify whether SFPD information is in fact a match to a watch list record.[59] Specific procedures and criteria for this validation process are sensitive or classified and not available in public documents. Contracted Customer Service Agents (CSA) receive calls from aircraft operators, route them to an available SFA, and coordinate the resolution of traveler issues which may entail instructing the airline to print a boarding pass or coordinate notification of local law enforcement for further involvement if necessary.[60]

Figure 2 represents the process flow for Secure Flight vetting, verification, and coordination procedures.

---

[57] U.S. Department of Homeland Security, Transportation Security Administration, Office of Acquisition. "Official Solicitation for the TSA Secure Flight Resolution Center, call center support." Solicitation No. HSTS02-08-R-TTC159. July 3, 2008. https://www.fbo.gov/index?tab=documents&tabmode=form&subtab=core&tabid=ed9d723a863da7938300737ab3358e07.

[58] Ibid.

[59] U.S. Department of Homeland Security, Office of Inspector General. *Implementation and Coordination of TSA's Secure Flight Program (redacted version*). (OIG-12-94) (Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

[60] U.S. Department of Homeland Security, Transportation Security Administration, Office of Acquisition. "Official Solicitation for the TSA Secure Flight Resolution Center, call center support." Solicitation No. HSTS02-08-R-TTC159. July 3, 2008. https://www.fbo.gov/index?tab=documents&tabmode=form&subtab=core&tabid=ed9d723a863da7938300737ab3358e07.

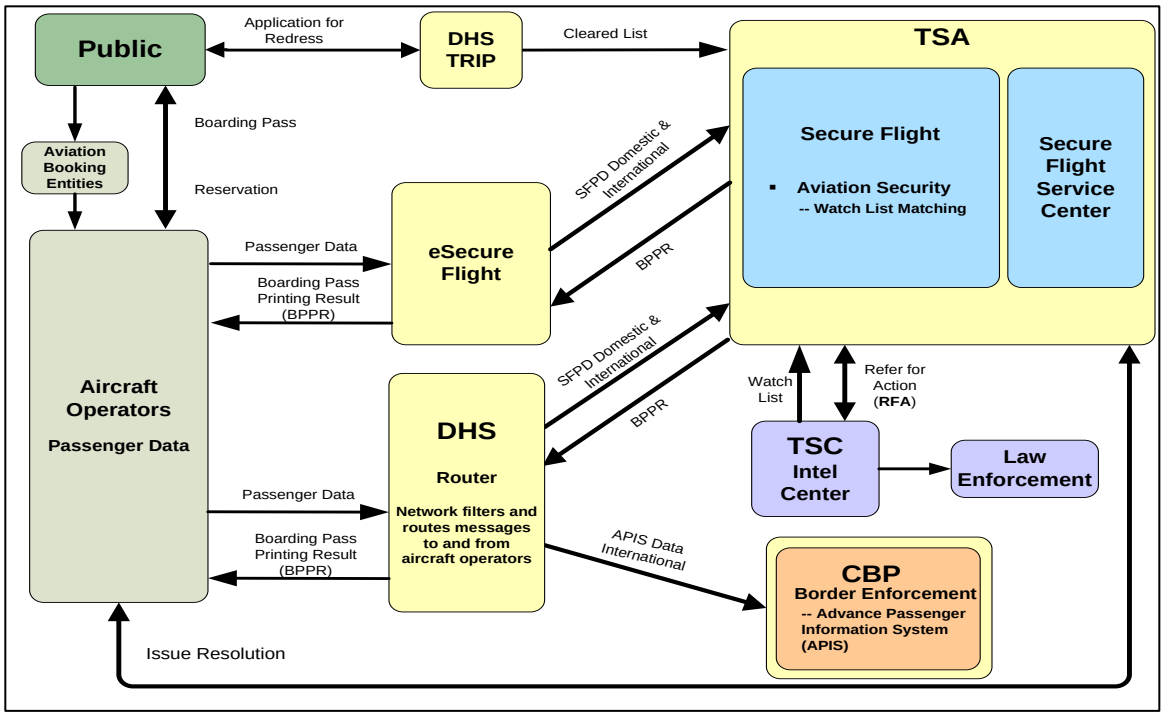

Figure 2. Secure Flight Procedures (from TSA, 2009.)[61]

There are weaknesses in this process. Federal Government and private industry partners have raised concerns that passengers can submit false data or present false identity documents to gain access to aircraft or "sterile areas of airports.[62] To address this concern, TSA and Secure Flight are developing technology to use boarding pass scanners to help authenticate identity documents to ensure that all SFPD information matches the information on an individual's identity document. This effort is called the Credential Authentication Technology – Boarding Pass Scanning Systems Initiative.[63]

---

[61] U.S. Department of Homeland Security, Transportation Security Administration. *Secure Flight: Your Safety is Our Priority*. As presented at the National Business Travel Association International Conference and Expo, San Diego, CA. August 26, 2009. http://www.gbta.org/Lists/Resource Library/Secure Flight Presentation.ppt.

[62] U.S. Department of Homeland Security, Office of Inspector General. *Implementation and Coordination of TSA's Secure Flight Program (redacted version*). (OIG-12-94) (Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

[63] U.S. Department of Homeland Security, Privacy Office. *Privacy Impact Assessment Update For Credential Authentication Technology/Boarding Pass Scanning System.* (DHS/TSA/PIA-024(b)) (Washington, DC: Department of Homeland Security, January 2013). http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia%20update_tsa_cat%20bpss_20130118.pdf.

False identities and false documents pose a problem for aviation security. As the GAO notes, "The Secure Flight Program relies on the accuracy of the information passengers submit during the reservation process."[64] This weakness to national security is further examined in the analysis section of this chapter.

1. Development Status and System Performance

The Secure Flight system has been developed and implemented incrementally. As DHS OIG noted in 2012:

> Secure Flight began program implementation with the first domestic aircraft operator on January 27, 2009. On June 22, 2010, Secure Flight met its goal of conducting watch list matching for all domestic aircraft operator flights within, into and out of the United States, as well as international point-to-point flights between two foreign cities. On November 23, 2010, Secure Flight completed deployment to all covered foreign air carriers flying into and out of the United States. Secure Flight expects all overflights (flights that fly over the United States, but do not land) will be covered by the end of calendar year 2012.[65]

Though enhancements and expansions of Secure Flight continue, the program is in the "support life cycle phase," according to the White House's "Federal IT Dashboard,"[66] which tracks and publishes information on large federal information technology investments. A typical information technology development life cycle includes design and development, acceptance testing, as well as training and transitioning as part of implementation. After deployment, the system is said to be in the "maintenance and operations" or "support" phase, as is the case with Secure Flight. This means that the system is fully operational with development or programming activities limited to maintenance and enhancements. TSA reports on the "IT Dashboard" that it has

---

[64] U.S. Department of Homeland Security, Office of Inspector General. *Implementation and Coordination of TSA's Secure Flight Program (redacted version*), (OIG-12-94) (Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

[65] U.S. Department of Homeland Security. *Annual Performance Report, Fiscal Years 2012 – 2014*. (Washington, DC: Department of Homeland Security, April 2013). http://www.dhs.gov/sites/default/files/publications/MGMT/DHS-%20Annual%20Performance%20Report%20and%20Congressional-Budget-Justification-FY2014.pdf.

[66] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=17. (Accessed May 26, 2014).

implemented enhancements to Secure Flight to support the Pre✔ program.[67] The TSA also reports that the "program continues to operate within acceptable ranges for cost and schedule variances."[68] The Department of Homeland Security (DHS) Chief Information Officer (CIO) continues to assess the Secure Flight program as a Moderately Low Risk investment."[69]

Technological systems, especially those that rely on connections between networks, sometimes experience disruptions or outages. To reduce disruptions, Secure Flight has operational and system redundancy[70] at Secure Flight centers in Annapolis Junction, Maryland and Colorado Springs, Colorado.[71] Operational statistics from the White House IT Dashboard report that the service availability of Secure Flight to process SFPD from airlines at one or the other operation center was 100% as of May 2014.[72]

The performance of the system as related to specific program goals will be evaluated in later sections.

D. ANALYSIS

In evaluating the appropriateness of the use of automation and DSS in the Secure Flight program, it is important to note that comprehensive, real-time passenger watch list matching would not be feasible without automation. Considering the volume of passengers checked—an estimated 2 million daily—this process could not exist without the use of pre-programmed matching queries of SFPD against the TDSB and other watch

---

[67] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=17. (Accessed May 26, 2014).

[68] Ibid.

[69] Ibid.

[70] U.S. Department of Homeland Security, Office of Inspector General. *Implementation and Coordination of TSA's Secure Flight Program (redacted version*), OIG-12-94, (Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

[71] U.S. Department of Homeland Security, Transportation Security Administration, Office of Acquisition. "Official Solicitation for the TSA Secure Flight Resolution Center, call center support." Solicitation No. HSTS02-08-R-TTC159. July 3, 2008. https://www.fbo.gov/index?tab=documents&tabmode=form&subtab=core&tabid=ed9d723a863da7938300737ab3358e07.

[72] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=17. (Accessed May 26, 2014).

lists. The procedures for watch list matching by the airlines prior to the implementation of Secure Flight likely involved the use of decision support or querying tools; it is not likely that names were manually entered into a system to compare against the terror watch lists. Analyses of the benefits and costs of the Secure Flight program are of the improvements, if any, that the Secure Flight system offers over decentralized, non-standardized matching by the airlines. It is well understood that prior to the implementation of Secure Flight, matching was completed using different methods and techniques by different airlines.[73] This establishes a baseline of performance for service, operational efficiencies, and national security to make a comparison for this analysis.

Unlike the airlines' automated procedures for querying passenger information before the implementation of Secure Flight, the current procedures for querying databases in immigration adjudication are almost entirely manual. Despite this difference, this analysis informs the evaluation of implementing automation or DSS for immigration adjudications. An analysis of the streamlining of matching procedures into a centralized system, of the benefits and costs to stakeholders, and of procedures for verifying matches manually and coordinating procedures with law enforcement or other partners can inform the decision to utilize automation and DSS for immigration adjudications.

1. Benefits and Costs to Stakeholders

This case study will attempt to identify and categorize expected and realized benefits and costs to the Secure Flight stakeholders. Secure Flight's primary stakeholder and customer is the traveling public. Another important group of stakeholders are commercial aircraft carriers in the aviation industry.

The use of DSS to vet passenger names against watch lists to automatically clear them, flag them, or refer those with adverse information for manual reviews offers several benefits to stakeholders. These include passenger-related customer service improvements and benefits that support airline industry business models. Automation/

[73] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management. *Regulatory and Economic Analysis. Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf .

DSS also offers national security benefits through risk reduction and direct operational efficiencies to the Agency. Many of the benefits of the Secure Flight program's automated watch list matching and its supporting procedures are interrelated and intertwined across stakeholders and categories.

a. Benefits to the Traveling Public

Benefits to the traveling public derived from the implementation of automated watch list matching include faster and more efficient processing, protection of passenger privacy, and an improved redress process for misidentified passengers. The enhancement of the security of commercial air travel is a direct benefit to passengers and will be discussed in detail in a later section.

Faster and More Efficient Processing

By implementing one watch list matching system, the Secure Flight program claims to "provide a fair and consistent matching process across all airlines and reduces the chance of being misidentified."[74] In evaluating the Secure Flight procedures and decision support tool, there is validity to this claim.

By bringing watch list matching under a single centralized system, Secure Flight indeed implements consistency across all aircraft operators[75] where previously there was variability. Whatever value the traveling public places on consistency, fairness, and equitability, Secure Flight offers an improvement.

Secure Flight also claims that its matching system is "more effective" and passengers benefit from fewer travelers misidentified.[76] The Secure Flight Communications Toolkit, available online, states: "Providing the required data elements enables Secure Flight to more effectively perform watch list matching. More than 99

---

[74] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Communications Toolkit: Talking Points for Editorial from TSA." July 20, 2010, Version 3.0. http://www.tsa.gov/content/communications-toolkit. (Accessed May 26, 2014).

[75] Ibid.

[76] U.S. Department of Homeland Security, *Advance Passenger Information System Pre-Departure Final Rule & Secure Flight Notice of Rule Making.* (Washington, DC: Department of Homeland Security, D.C.: n.d.). http://www.hlswatch.com/sitedocs/apis-secure-flight-joint-faqs.pdf.

percent of passengers will be cleared to print their boarding passes at home when complete information is provided."[77] Though the statistic cannot be evaluated without testing the system, this claim also has validity. Although Secure Flight requires that passengers provide more data –technically a "cost" to them—the collection of additional data elements enables more reliable matching results. Fewer false positives mean fewer passengers are misidentified. This reduces the probability of a passenger being selected for expedited screening and is an improvement over prior matching systems and procedures.

Fewer false negatives mean that matches to the watch lists are more consistently identified. The robustness of the queries and the use of additional data elements improves matching, thus supporting Secure Flight's claim of improvements to security for the traveling public.[78] More analysis of improvements to national security is offered in a later section.

TSA also claims that Secure Flight offers a "better travel experience for passengers"[79] because it performs watch list matching prior to the passengers arriving at the airport. There is validity to this claim due to the accompanying validation procedures. Because Secure Flight requires the submission of available data 72 hours before scheduled departure,[80] SFA have the opportunity to investigate the potential matches and clear false positives, if possible. This would certainly reduce or eliminate the inconvenience for a passenger who was initially matched to a list, but cleared in advance

[77] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Communications Toolkit: Talking Points for Editorial from TSA." July 20, 2010, Version 3.0. http://www.tsa.gov/content/communications-toolkit. (Accessed May 26, 2014).

[78] U.S. Department of Homeland Security, *Advance Passenger Information System Pre-Departure Final Rule & Secure Flight Notice of Rule Making.* (Washington, DC.: Department of Homeland Security, n.d.). http://www.hlswatch.com/sitedocs/apis-secure-flight-joint-faqs.pdf.

[79] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Communications Toolkit: Talking Points for Editorial from TSA." July 20, 2010, Version 3.0. http://www.tsa.gov/content/communications-toolkit. (Accessed May 26, 2014).

[80] Delta Airlines. "Secure Flight Passenger Data (SFPD) FAQs." October 8, 2010. http://www.delta.com/content/www/en_US/agency/useful-resources/secure-flight-passenger-data-faqs.html. (Accessed May 22, 2014).

of a flight. In addition, uniform watch list matching conducted prior to boarding reduces or eliminates the potential for flight diversions or deplaning due to watch list concerns.[81]

Figure 3 depicts TSA's vision for the Secure Flight program.

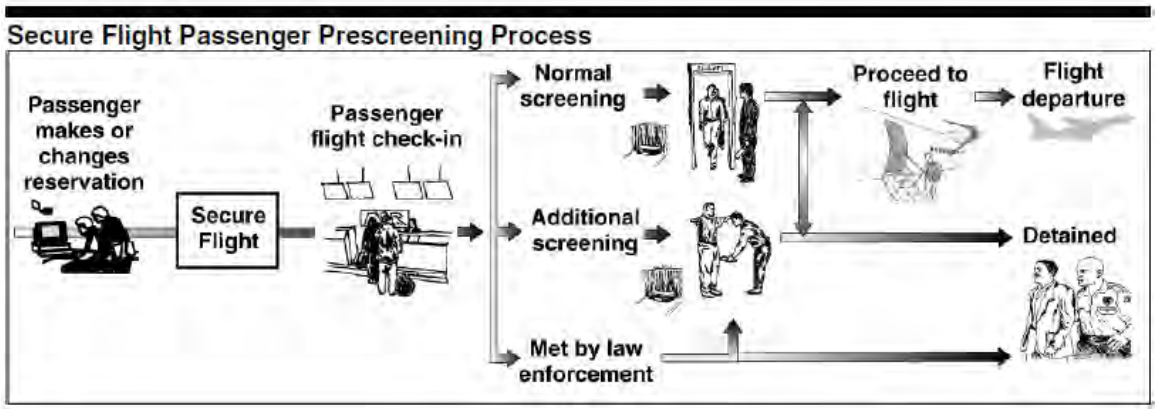

Figure 3. Secure Flight Passenger Procedures (from GAO, 2005)[82]

Protecting Passenger Privacy

Prior to the implementation of Secure Flight, aircraft operators performed passenger name matching against copies of terrorist watch lists. Details on each airline's procedures for watch list matching are not available, but these procedures likely did not involve transmission of data—which carries information security and privacy risks. That being said, the lack of centralization or regulation in watch list matching means that individual airline procedures were certainly different, and thus the handling of passenger information was inconsistent.

"Protecting the privacy of individuals' information is a cornerstone of Secure Flight,"[83] states the TSA website providing Secure Flight program information. The

[81] U.S. Department of Homeland Security. *Advance Passenger Information System Pre-Departure Final Rule & Secure Flight Notice of Rule Making*. (Washington, DC: Department of Homeland Security, n.d.). http://www.hlswatch.com/sitedocs/apis-secure-flight-joint-faqs.pdf.

[82] U.S. Government Accountability Office. *Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed*. (GAO-05-256) (Washington, DC: GPO, 2005). http://www.gao.gov/products/GAO-05-256.

Privacy Act of 1974 "prohibits the disclosure of a record about an individual"[84] from any government system of records without his/her written consent, "unless the disclosure is pursuant to one of twelve statutory exceptions."[85] Privacy Act regulations required that the Secure Flight program file a System of Records Notice (SORN)[86] as well as regular updates to a Privacy Impact Analysis (PIA).[87] TSA simultaneously filed a rulemaking to exempt Secure Flight from certain provisions of the Privacy Act. Those provisions related to protecting counterterrorism, law enforcement, or intelligence investigations and analysis activities.[88] As a result, Secure Flight's "cornerstone" of privacy—that passenger information is protected and not released to the general public—must be interpreted to include the use of that information for other purposes, such as counterterrorism, law enforcement, or intelligence.

TSA states that all "personal data is collected, used, distributed, stored and disposed of in accordance with stringent guidelines and all applicable privacy laws and regulations."[89] Adherence to Privacy Act regulations is intended to protect passengers' personal information from unauthorized use and disclosure.[90] GAO has documented that privacy experts were involved in system development. GAO also notes that TSA has implemented training for Secure Flight staff in privacy policies and procedures and has privacy performance metrics and analyses. TSA is credited with implementing controls

---

[83] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Overview." March 19, 2014.,http://www.tsa.gov/stakeholders/secure-flight-program. (Accessed May 26, 2014).

[84] *Privacy Act, U.S. Code 5* (1974), § 522a. http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf.

[85] Ibid.

[86] The Privacy Act of 1974 requires agencies to publish a notice describing a record system from which information is retrieved by name or other personal identifier (such as Social Security Number) whenever such a system is created or substantially revised.

[87] The E-Government Act of 2002 requires agencies to conduct privacy impact assessment before developing systems that collect, maintain or disseminate information in an identifiable form.

[88] "Privacy Act of 1974: Implementation of Exemptions and System of Records; Secure Flight Records; Final Rule and Notice." *Federal Register* 7, no. 217 (Friday, November 9, 2007), 63706. http://www.gpo.gov/fdsys/pkg/FR-2007-11-09/pdf/E7-21907.pdf.

[89] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Overview." March 19, 2014. http://www.tsa.gov/stakeholders/secure-flight-program.

[90] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=17. (Accessed May 26, 2014).

for data quality, security, and access as well as other efforts to track and audit access to personally identifiable information (PII) in order to ensure passenger privacy.[91]

TSA asserts that it "collects the minimum amount of personal information necessary to conduct effective watch list matching."[92] However, for most airlines, the standard SFPD included more personal information than had previously been collected[93] and could be considered a negative impact on passenger privacy. Operational testing prior to the implementation of Secure Flight determined that it was necessary to standardize SFPD to include gender and birthdate for all passengers to minimize false positives and the subsequent inconvenience for legitimate passengers and to reduce the expenditure of resources to invalidate inappropriate matches.

As stated on an airline's website, customers must provide SPFD to be issued a boarding pass: "As a customer, you consent to the use of your Secure Flight information for these purposes."[94] On August 23, 2007, TSA issued a "Notice of Public Rule Making" (NPRM) to establish the Secure Flight Program[95] and another to exempt Secure Flight from certain provisions of the Privacy Act,[96] each with a 60-day open public comment period through October 22, 2007. On the same day, TSA also published a

---

[91] U.S. Government Accountability Office. *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks.* (GAO-09–292) (Washington, DC: GPO, 2009). http://www.gao.gov/products/GAO-09-292.

[92] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight: Frequently Asked Questions." March 19, 2014. http://www.tsa.gov/content/frequently-asked-questions-secure-flight.

[93] U.S. Department of Homeland Security, Office of Inspector General. *Implementation and Coordination of TSA's Secure Flight Program (redacted version*). (OIG-12-94) (Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

[94] United Airlines. "Secure Flight." http://www.united.com/web/en-US/content/travel/airport/id/secure.aspx.. (Accessed May 21, 2014).

[95] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Program." *Federal Register* 72, no. 163 (August 23, 2007): 48356. http://www.gpo.gov/fdsys/pkg/FR-2007-08-23/pdf/E7-15960.pdf.

[96] U.S. Department of Homeland Security, Transportation Security Administration. "Privacy Act of 1974: Implementation of Exemptions; Secure Flight Records." *Federal Register* 72, no. 163 (August 23, 2007): 48357, August 23, 2007. http://www.gpo.gov/fdsys/pkg/FR-2007-08-23/pdf/E7-15963.pdf.

"Privacy Impact Assessment" per Privacy Act requirements.[97] TSA received influential comments from two privacy advocacy groups related to the collection and storage of SFPD and to a concern about the efficacy of redress processes.[98] In its response, TSA continued to claim a need for certain exemptions for national security and law enforcement purposes.[99] Secure Flight thus acknowledges that it is exercising a privacy tradeoff for improved matching efficiency. This tradeoff may be mitigated by the additional privacy protocols that TSA can enforce, but this mitigation may not satisfy privacy advocacy organizations.

Public communications such as an ad from TSA shown in Figure 4 are intended to inform passengers of the benefits of providing SFPD for Secure Flight Matching.

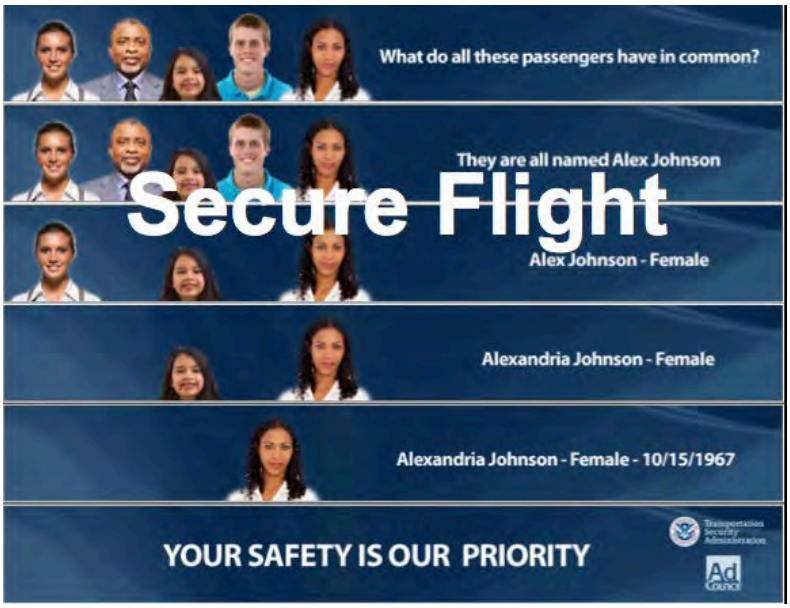

Figure 4. Secure Flight Ad (from GBTA, 2009)[100]

[97] U.S. Department of Homeland Security, Office of Privacy. "Privacy Impact Assessment." (Washington, DC: Department of Homeland Security, April 9, 2007). http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight.pdf.

[98] "Privacy Act of 1974: Implementation of Exemptions and System of Records; Secure Flight Records; Final Rule and Notice." *Federal Register* 7, no. 217 (Friday, November 9, 2007), 63706. http://www.gpo.gov/fdsys/pkg/FR-2007-11-09/pdf/E7-21907.pdf.

[99] Ibid.

[100] U.S. Department of Homeland Security Transportation Security Administration. "Secure Flight: Your Safety is our Priority." Presentation to Global Business Travel Association (GBTA) Conference, April 22, 2009. http://www.gbta.org/Lists/Resource%20Library/NBTAWebinar_SecureFlight.pdf .

Assertions that Secure Flight offers improvements to protecting the privacy of airline passengers over the previous system in which aircraft operators conducted watch list matching requires that independent reviewers confirm that TSA's privacy controls are effective. In 2006, the DHS Privacy Office reported some "largely unintentional, yet significant privacy missteps"[101] by the Secure Flight program in its operational testing and development phases. As a result, Secure Flight made significant changes in program requirements to address these privacy and security concerns.[102] In 2009, GAO documented privacy and security weaknesses in the Secure Flight program; however later that same year, it noted that TSA had "completed the actions to implement"[103] recommendations related to privacy and security, and it considered those conditions to be "generally achieved."[104] On May 21, 2014, the White House's "Federal IT Dashboard" analyzed Secure Flight to be in 100% compliance with privacy and records retention schedules as established by the National Archives and Records Administration (NARA).[105]

Improved redress process for passengers who have been misidentified

"Redress" refers to passenger-initiated corrections to watch list match results. Though the Secure Flight system intends to be an improvement in efficiency of watch list matching, "false positives" may still occur if a passenger has the same or similar name to someone on the watch list.[106] When a passenger's SFPD has produced a watch list match incorrectly, that individual may participate in the DHS Traveler Redress Inquiry Program

---

[101] U.S. Department of Homeland Security, Privacy Office. "Report to the Public on the Transportation Security Administration's Secure Flight Program and Privacy Recommendations." (Washington, DC: Department of Homeland Security, December 2006). http://www.dhs.gov/xlibrary/assets/privacy/privacy-secure-flight-122006.pdf.

[102] U.S. Government Accountability Office. *Assessments of Selected Complex Acquisitions*. (GAO-10-588SP) (Washington, DC: GPO, 2010). http://www.gao.gov/assets/210/204132.pdf.

[103] U.S. Government Accountability Office. *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks.* (GAO-09–292) (Washington, DC: GPO, 2009). http://www.gao.gov/products/GAO-09-292.

[104] Ibid.

[105] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=172. (Accessed May 26, 2014).

[106] NBS News.com, "How Secure Flight Works." http://www.nbcnews.com/id/39892975/ns/travel-travel_tips/t/how-secure-flight-works/. (Accessed June 1, 2014).

(DHS TRIP). It serves as a "single portal for travelers to seek redress for adverse screening experiences and to resolve possible watch list misidentification issues."[107] Prior to the implementation of Secure Flight, individuals seeking redress had limited success in airlines recognizing their redress credential due to the diversity of matching systems.[108]

Secure Flight states that it uniformly applies the DHS TRIP list in its watch list matching process to prevent the misidentification of passengers who have been cleared.[109] Operational performance statistics from the White House IT Dashboard reported that 99.96 percent of passengers who have submitted a valid redress number have been automatically recognized and cleared by the Secure Flight system. The target for 2014 was 95 percent.[110] Although this implies that the system is working well and is an improvement for many passengers, nevertheless it still means that many are not recognized and continue to face enhanced screening or other difficulties when they attempt to fly. The DHS TRIP program including application procedures and processing time have come under review by the DHS OIG.[111] Improvements to this program would directly improve Secure Flight.

b. Costs to the Traveling Public

Compliance with data collection requirements

TSA claims "it is to the passenger's advantage to provide the required data elements" to prevent delays or inconveniences at the airport, "particularly for those

---

[107] Ibid.

[108] U.S. Department of Homeland Security Transportation Security Administration. "Secure Flight: Your Safety is our Priority." Presentation to NBTA Conference, April 22, 2009. http://www.gbta.org/Lists/Resource%20Library/NBTAWebinar_SecureFlight.pdf .

[109] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Communications Toolkit: Talking Points for Editorial from TSA." July 20, 2010, Version 3.0. http://www.tsa.gov/content/communications-toolkit. (Accessed May 26, 2014).

[110] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=17. (Accessed May 26, 2014).

[111] U.S. Department of Homeland Security, Office of Inspector General. *Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program (redacted version).* (OIG-09-103) (Washington, DC: Department of Homeland Security, September 2009). http://www.oig.dhs.gov/assets/Mgmt/OIG-09-103r_Sep09.pdf .

individuals who have been misidentified in the past."[112] This claim is likely valid for individuals who were incorrectly matched to a watch list prior to Secure Flight but were properly cleared since its implementation. However, for most passengers who never matched to a list, providing additional information about themselves to comply with SFPD requirements could be considered an opportunity cost with no direct benefit.

That being said, the amount of time to provide this data could conceivably be discounted as negligible. For a technology savvy individual who has made flight reservations on an airline's website, completing a few additional fields might amount to a few seconds. In the Regulatory and Economic Analysis prepared by TSA's Transportation Sector Network Management (TSNM) group, the amount of additional time to provide this information was estimated between 10 and 25 seconds depending on the mode of reservation.[113] Aggregated over the millions of flights to, from, or within the United States, however, this time represents a significant cost. The TSNM analysis estimates this cost would amount to $645.6 million over the first 10 years of the program, based on hourly rate guidance from TSA and estimates on the number of flights subject to the Secure Flight rule.[114]

Personal privacy concessions

As previously discussed in the traveler benefits section, opinions on Secure Flight's impact on passenger privacy are mixed. Privacy advocacy organization Electronic Frontier Foundation (EFF)[115] submitted comments in September 2007, shortly after the NPRM request to exempt Secure Flight from certain provisions of the Privacy Act. EFF generally challenged TSA's bases for claiming Privacy Act exemptions, stating

---

[112] NBS News.com, "How Secure Flight Works." http://www.nbcnews.com/id/39892975/ns/travel-travel_tips/t/how-secure-flight-works/. (Accessed June 1, 2014).

[113] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management, *Regulatory and Economic Analysis. Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

[114] Ibid.

[115] Electronic Frontier Foundation. "Comments of the Electronic Frontier Foundation." September 24, 2007. https://www.eff.org/files/filenode/travelscreening/092407_secure_flight_comments.pdf. (Accessed July 25, 2014).

that the Secure Flight program "lacked adequate transparency" and failed to assure the public that their information would only be collected for "relevant and necessary use."[116] EFF further claimed that Secure Flight provides individuals neither a "meaningful redress process" nor "meaningful access to personal information."[117] The DHS TRIP program had only recently been established at the time of the NPRM, and its development maturation may satisfy EFF's concerns about redress. Though TSA countered these comments in their response,[118] they remain valid.

c. Benefits to the Aviation Industry

Relief from watch list matching responsibilities

The most tangible benefit to the air carriers is that, with the full implementation of the Secure Flight program, they are relieved of the responsibility for watch list matching.[119] Elimination of watch list matching responsibilities enables airlines to reallocate some operational resources to core business or other tasks and offset some of the costs incurred to comply with Secure Flight regulations.[120] These costs will be discussed further.

Match resolution

The majority of aircraft operators interviewed by the OIG noted a "decrease in the average resolution call time since Secure Flight's implementation. The average call response time for FY 2011 was 7 seconds with most resolution calls lasting 2 to 8

---

[116] Ibid.

[117] Ibid.

[118] "Privacy Act of 1974: Implementation of Exemptions and System of Records; Secure Flight Records; Final Rule and Notice." *Federal Register* 7, no. 217 (Friday, November 9, 2007), 63706. http://www.gpo.gov/fdsys/pkg/FR-2007-11-09/pdf/E7-21907.pdf .

[119] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management. *Regulatory and Economic Analysis. Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

[120] Ibid.

minutes;" however, a TSA customer service representative will "stay on the call as long as necessary to resolve any issues."[121]

d. Costs to the Airline Industry

As previously discussed, aircraft operators and travel agencies must submit SFPD electronically to Secure Flight. Most transmit passenger data directly through a DHS portal, and others submit data through the web application "eSecure Flight." Aircraft carriers had both initial and recurring costs to support this requirement. These costs generally take two forms: reprogramming costs and program implementation costs.[122]

Reprogramming includes such tasks as reprogramming the airline website to enable passengers to enter each component of their full name in a separate field; adding fields for date of birth, gender, and Redress Number, as necessary; and adding the privacy notice to websites. Additional reprogramming requirements include modifying ticketing consoles and kiosks to accept and properly process the gate and boarding pass printing instructions returned by Secure Flight.

The airlines had to change their systems and procedures to collect and submit SFPD. TSA determined the SFPD data elements required during the testing that was conducted prior to implementing Secure Flight. Airlines had been collecting information from passengers at the time of their reservations, but there was no consistency in the formats or elements collected across the airlines. Most were collecting less than what was determined to comprise SFPD.[123] Thus, upgrading reservation systems to capture all the

---

[121] U.S. Department of Homeland Security, Office of Inspector General. *Implementation and Coordination of TSA's Secure Flight Program (redacted version*). (OIG-12-94) (Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

[122] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management, *Regulatory and Economic Analysis. Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

[123] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management, *Regulatory and Economic Analysis. Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

SFPD elements, rebuilding collection tools, and retraining staff on the updated software and reservation procedures are all among the costs to the airlines and travel agencies.[124]

In an economic analysis, TSA's Transportation Network Management Office attempted to estimate the dollar costs associated with reprogramming and implementing systems to support Secure Flight. TSA encountered a wide variance in costs reported by airlines; however, they provide $1.5 million as an average per airline.[125] Full life-cycle costs are not presented in this analysis; however, recurring costs to support the Secure Flight program are expected. External sources have attempted to estimate the full cost of reprogramming airline and travel agency systems to be compliant with Secure Flight. The International Air Transport Association estimates that it will take $2 billion[126] to comply, and travel writer Edward Hasbrouck has estimated the industry will bear a $1 billion burden.[127]

Additionally, the airlines have borne much of the burden associated with customer awareness campaigns. The traveling public likely became aware of the new requirements for SFPD the first time they made an airline reservation after the implementation of Secure Flight. Airlines had to provide additional information and undoubtedly had to field customer service inquiries from passengers when the changes went into effect. Indeed, all major U.S. carriers, such as United Airlines,[128] American Airlines,[129] and

---

[124] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management, *Regulatory and Economic Analysis. Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

[125] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management, *Regulatory and Economic Analysis. Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

[126] American Civil Liberties Union (ACLU). "The Four Biggest Problems With the 'Secure Flight' Airline Security Program." March 4, 2005. https://www.aclu.org/technology-and-liberty/four-biggest-problems-secure-flight-airline-security-program. (Accessed May 25, 2014).

[127] Edward Hasbrouck. "Why CAPPS-II Would Cost a Billion Dollars." *The Practical Nomad*, February 13, 2004. http://hasbrouck.org/blog/archives/000149.html .

[128] United Airlines. "Secure Flight." http://www.united.com/web/en-US/content/travel/airport/id/secure.aspx. (Accessed May 21, 2014).

[129] American Airlines. "TSA Secure Flight Information Is Required To Travel." n.d. http://www.aa.com/i18n/utility/secureFlight.jsp?anchorLocation=DirectURL&title=secureflight. (Accessed May 25, 2014).

Delta,[130] have specific information posted on their websites related to Secure Flight. Most of these websites reflect content that TSA produced in a "toolkit" specifically for airlines to communicate to their customers.[131] This may have decreased the communication burden on airlines; however, the airlines remain the "front line" of customer service related to Secure Flight.

TSA reported to the White House IT Dashboard that 100 percent of the aircraft operators that were covered under the Secure Flight Final Rule had "on-boarded" with the program, and that 98.54 percent of all SFPD submissions were compliant.[132] This indicates that most airlines have already incurred the costs of implementing the system and are now in the "recurring costs" phase of supporting the program. While the airline industry has struggled in recent years, compliance with Secure Flight has not been cited as a reason for airline challenges.

2. Benefits and Costs to Agency Operations

a. Benefits to Operations

Resource alignment

Reliability and efficiency in automation refer to a model performing within a specified margin of error—that is, does it minimize false positives and false negatives. While neither the error statistics nor the matching criteria for Secure Flight are available in public documents, significant testing went into the development of the model and the required data elements. The OIG and GAO reports indicate that Secure Flight continues refining the matching criteria to ensure that the system appropriately identifies those who match a watch list and clear those who do not. In addition to continuously refined queries, the incorporation of data from the DHS TRIP and "Trusted Traveler" programs,

---

[130] Delta Airlines. "Secure Flight Passenger Data (SFPD) FAQs." October 8, 2010. http://www.delta.com/content/www/en_US/agency/useful-resources/secure-flight-passenger-data-faqs.html. (Accessed May 25, 2014).

[131] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Communications Toolkit: Talking Points for Editorial from TSA." July 20, 2010, Version 3.0 http://www.tsa.gov/content/communications-toolkit. (Accessed June 1, 2014).

[132] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=172. (Accessed May 26, 2014).

such as Global Entry, SENTRI and NEXUS,[133] improve the reliability and robustness of the matching results. This allows for a more optimal allocation of resources. For example, positive matches require review by an SFA and potentially enhanced security screening. Fewer false positives and negatives reduce the instances that require labor-intensive review. This results in improved overall operational efficiency.[134] This efficiency benefits TSA and partners who may be involved in labor-intensive processes, such as law enforcement or the airlines.

Alerts and referral procedures

The Secure Flight Program automation tool and procedures may provide earlier insight into potential matches, improving the coordination of response activities. For all advance reservations, Secure Flight requires that passenger data be sent for matching purposes 72 hours before a departure.[135] Secure Flight's automated, rapid results and preliminary notification reports on potential matches allows for manual verification by an SFA before a scheduled flight. This also expedites law enforcement notification[136] and allows federal entities to coordinate coverage at airports and on aircraft, as necessary.[137] Prior to the implementation of Secure Flight, the coordination of law enforcement or other necessary response to a potential match was not consistent across the aviation industry.[138] SF also provides an interactive capability for recurring or manual watch list matching on a 24/7 basis through the SF Operations Center. "[139]

---

[133] United Airlines. "Secure Flight." http://www.united.com/web/en-US/content/travel/airport/id/secure.aspx. (Accessed May 21, 2014).

[134] NBS News.com, "How Secure Flight Works," http://www.nbcnews.com/id/39892975/ns/travel-travel_tips/t/how-secure-flight-works/. (Accessed June 1, 2014).

[135] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=172. (Accessed May 26, 2014).

[136] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight: Your Safety is our Priority." Presentation to NBTA Conference, April 22, 2009. http://www.gbta.org/Lists/Resource%20Library/NBTAWebinar_SecureFlight.pdf .

[137] U.S. Department of Homeland Security, Office of Inspector General. *Implementation and Coordination of TSA's Secure Flight Program (redacted version*), (OIG-12-94) (Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

[138] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=172. (Accessed May 26, 2014).

[139] Ibid.

Secure Flight also enables risk-based initiatives such as expedited airport screening procedures for passengers who are identified as "low-risk." Discussed later as it relates to national security benefits, utilizing the information from Secure Flight on a passenger's relative security risk could improve airport screening operations by enabling TSA to focus its resources on higher-risk passengers.[140]

b. Costs to Operations

Costs of Development, Maintenance, and Operations

It is important to note that federal operation of watch list matching and development of the Secure Flight program were mandated by Congress through IRTPA 2004.[141] An analysis of alternatives that is generally required for large-scale federal acquisitions was not conducted. However, the costs to develop and maintain the system have been systematically reviewed and scrutinized by several organizations, including GAO, both DHS and Department of Justice OIG, and the White House information technology review panel called the IT Dashboard.

Compiling the numbers published by any of these organizations is difficult and would not likely yield an accurate aggregation or total estimated cost for implementing and operating Secure Flight. During the five-year period in which TSA began building and testing Secure Flight, it received appropriations of approximately $300 million.[142]

Maintenance, operations, and enhancement costs for Secure Flight remain high. Figure 5, a chart produced by GAO, demonstrates the continuing costs to support the Secure Flight effort as reported by DHS:

---

[140] U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management. *Regulatory and Economic Analysis. Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560).* October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

[141] Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA). Pub. L. No. 108–458, 118 Stat. 3638 (Dec. 17, 2004), codified at 42 U.S.C. §2000ee, 50 U.S.C. §403-1 et seq., §403-3 et seq., §404o et. seq.

[142] U.S. Government Accountability Office. *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks*. (GAO-09–292) (Washington, DC: GPO, 2009). http://www.gao.gov/products/GAO-09-292.

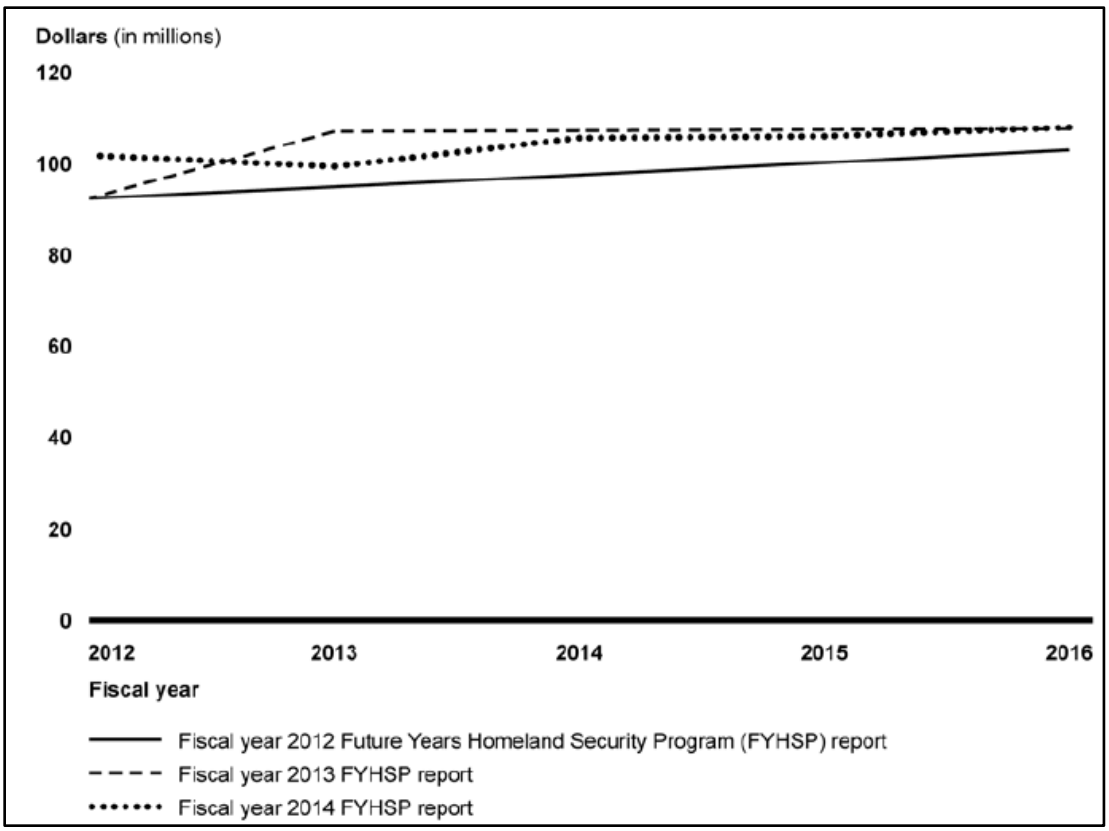

Figure 5. GAO Analysis of Secure Flight Continuing Costs (from GAO, 2014)[143]

These costs appear to rise over time; however, it is difficult to differentiate maintenance costs from enhancement costs. The success of the Secure Flight program has resulted in its continued development and the expansion of its capabilities from its initial deployment. For example, TSA's fiscal year 2012 budget request proposed funding to deploy a pilot project related to screening against the additional TSDB records.[144] This included an increase of $8.9 million and 38 full-time personnel that TSA stated it would use for "information technology enhancements that will be required to implement this expanded screening and will allow TSA to handle the increased workload."[145]

[143] U.S. Government Accountability Office. *Homeland Security Acquisitions: DHS Could Better Manage Its Portfolio to Address Funding Gaps and Improve Communications with Congress.* (GAO-14-332) (Washington, DC: GPO, 2014). http://www.gao.gov/products/GAO-14-332.

[144] U.S. Government Accountability Office. *Terrorist Watchlist: Routinely Assessing Impacts of Agency Actions since the December 25, 2009, Attempted Attack Could Help Inform Future Efforts*. (GAO-12-476) (Washington, DC: GPO, 2012). http://www.gao.gov/assets/600/591312.pdf .

[145] Ibid.

Another budget request included $12.7 million for fully deploying the Secure Flight system over all passengers as mandated by IRTPA which TSA stated would add "a significant layer to TSA's aviation security operations."[146] TSA requested an additional $30 million for a Technology Infrastructure Modernization (TIM) program that was intended to "achieve significant economies of scale and other benefits associated with a unifying business integration effort."[147] TSA's overall budget request to support Secure Flight grew from $92,414,000 and 239 government full-time equivalent (FTE) employees in fiscal year 2012[148] to $106,198,000 and 286 FTE in fiscal year 2014.[149]

To support the Secure Flight Program, the FBI's Terrorist Screening Center (TSC) made systems and procedures changes. According to the Department of Justice Office of the Inspector General (DOJ OIG), the direct and indirect costs associated with this effort in 2005 and 2006 exceeded $58 million.[150] Operations expenses continue for the TSC, as well.

As previously mentioned, these costs are appropriated by the Congress to support this federally mandated program. If the demonstrated value of the Secure Flight program was not apparent to the Congress, it would have the opportunity to decline budget requests.

The GAO and DHS OIG have both identified cost and schedule risks associated with the management of the Secure Flight program in several reports ranging from 2008

---

146 U.S. Department of Homeland Security. *Budget-in-Brief, Fiscal Year 2014.* (Washington, DC: Department of Homeland Security, February 2013). http://www.dhs.gov/sites/default/files/publications/MGMT/FY%202014%20BIB%20-%20FINAL%20-508%20Formatted%20%284%29.pdf.

147 Ibid.

148 U.S. Department of Homeland Security. *Annual Performance Report Fiscal Years 2012–2014.* (Washington, DC: Department of Homeland Security, 2013). http://www.dhs.gov/sites/default/files/publications/MGMT/DHS-%20Annual%20Performance%20Report%20and%20Congressional-Budget-Justification-FY2014.pdf.

149 Ibid.

150 U.S. Department of Justice, Inspector General. *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program (redacted version).* (OIG-05-34) (Washington, DC: Department of Homeland Security, 2005). http://www.justice.gov/oig/reports/FBI/a0534/final.pdf.

to the present.[151] Efficient and effective management of resources would limit the unnecessary cost associated with maintaining and enhancing the Secure Flight system.

3. Effects of Automation on National Security

a. Benefits to National Security

> The matching of airline passenger information against terrorist watch-list records (watch-list matching) is a frontline defense against acts of terrorism that target the nation's civil aviation system.[152]

Centralized automated operations: consistency, uniformity, and flexibility

As discussed, before the implementation of Secure Flight, airlines were responsible for performing watch list matching of passengers with a variety of systems and procedures.[153] By assigning the watch list screening process to the federal government, procedures are consistent across all airlines, and comparisons can be made using a single system.[154] This benefits national security.

First, it allows SFA to develop expertise with results to better identify potential issues. The analysis of results to confirm a match is one of the most important steps in the process from a national security perspective. The automated matching tool is a "decision support" system in that it is intended to clear from the queue most individuals who are very unlikely to pose a threat based on the query logic. Certainly, the appropriateness of the logic and the quality of the data are also significant factors in national security, both to be addressed later in this section. By uniformly applying the logic across all airlines,

---

[151] See U.S. Government Accountability Office reports GAO-06-864T, GAO-09-29, GAO-14-332. Available at http://www.gao.gov/index.html . See also U.S. Department of Homeland Security, Office of the Inspector General, report OIG-12-94, available at http://www.oig.dhs.gov.

[152] U.S. Government Accountability Office. *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks*. (GAO-09–292) (Washington, DC: GPO, 2009). http://www.gao.gov/products/GAO-09-292.

[153] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=172. (Accessed May 26, 2014).

[154] U.S. Government Accountability Office. *Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program*. (GAO-06-864T) (Washington, DC: GPO, 2006). http://www.gao.gov/products/GAO-06-864T.

the SFA is given the opportunity to develop expertise in the matching process to better identify potential issues.

Additionally, the system can be "effectively and swiftly calibrated"[155] with changes applied universally across all passengers and airlines. This can be done either temporarily in response to an elevated threat environment, or permanently, based on new information or analysis to improve matching logic. This applies to both procedures and technologies. Flexibility and rapid responsiveness in watch list matching have a positive effect on national security. Both are improved by centralized, automated systems and operations.

Use of real-time and expanded watch lists

National security is improved by centralizing the watch list matching procedures in the federal government by improving the quality of the input data. That is, the federal government can connect directly to the TDSB and utilize real-time watch list information,[156] whereas previously, aircraft operators might have been using a list that was out of date. Further, if needed, the federal government can authorize the inclusion of additional or expanded lists in real time to vet potential matches or apply to all passengers when warranted by security considerations,[157] for example, if TSA learns that flights on a particular route may be subject to increased security risk.[158] The use of a centralized watch list matching decision support system enables improvements to national security that were unavailable under the previous system.

The quality of watch list data remains a criticism of the watch list matching process. The GAO has identified several issues related to watch list management in its

---

[155] U.S. Department of Homeland Security, *Advance Passenger Information System Pre-Departure Final Rule & Secure Flight Notice of Rule Making.* (Washington, DC: Department of Homeland Security, n.d.). http://www.hlswatch.com/sitedocs/apis-secure-flight-joint-faqs.pdf.

[156] Ibid.

[157] U.S. Government Accountability Office. *Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program.* (GAO-06-864T) (Washington, DC: GPO, 2006). http://www.gao.gov/products/GAO-06-864T.

[158] U.S. Government Accountability Office. *Terror Watchlist: Routinely Assessing Impacts of Agency Actions since the December 25, 2009, Attempted Attack Could Help Inform Future Efforts*. (GAO-12-476) (Washington, DC: GPO, 2012). http://www.gao.gov/assets/600/591312.pdf.

oversight of the Terrorism Screening Center (TSC), especially after the failure to accurately identify and prevent Umar Farouk Abdulmutallab—often referred to as "the underwear bomber"—from boarding Northwest Airlines Flight 253 from Amsterdam to Detroit, where he attempted to detonate a concealed explosive device on December 25, 2009.[159] The American Civil Liberties Union (ACLU) criticized the lists in 2005, citing "disastrous"[160] experiences that Americans have had being misidentified. Though presumably the DHS TRIP program corrects many of the issues cited by the ACLU, poor data quality would certainly affect the quality of watch list matches. The quality of the nomination process and the information stored in the TDSB is managed and reviewed by separate processes and is not affected—at least initially—by the use of Secure Flight.

At first implementation, this risk to national security related to watch list data quality *at a minimum does not increase* with the use of Secure Flight DSS and automation. It is reasonable to suspect that feedback loops between TSA and TSC could enable improvements to data quality in the TDSB. The sharing of PII across agencies requires adherence to privacy regulations to ensure that it is handled properly and utilized only for national security or law enforcement purposes.[161] Information collected by TSA through redress checks or manual vetting by an SFA, if fed back to the TDSB, could improve national security efforts beyond aviation security.

Expediting law enforcement response

Perhaps one of the most important benefits of the Secure Flight system and procedures is the improved ability to coordinate an appropriate law enforcement response to potential threats.[162] The Secure Flight system provides earlier insight to potential

---

[159] U.S. Government Accountability Office. *Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program*. (GAO-12-476) (Washington, DC: GPO, 2012). http://www.gao.gov/assets/600/591312.pdf.

[160] American Civil Liberties Union (ACLU). "The Four Biggest Problems With the 'Secure Flight' Airline Security Program." March 4, 2005. https://www.aclu.org/technology-and-liberty/four-biggest-problems-secure-flight-airline-security-program. (Accessed May 25, 2014).

[161] Under 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2), an agency may exempt from certain provisions of the Privacy Act a system of records containing investigatory material.

[162] U.S. Department of Homeland Security. *Advance Passenger Information System Pre-Departure Final Rule & Secure Flight Notice of Rule Making.* (Washington, DC: Department of Homeland Security, n.d.). http://www.hlswatch.com/sitedocs/apis-secure-flight-joint-faqs.pdf.

matches due to efficient, automated matching.[163] After an automated match is made, the supporting procedures enable officials to address security threats sooner, improving the safety of air travel.[164] The timeliness and accuracy of matching and the ability to coordinate law enforcement responses were not consistent across the aviation industry[165] prior to the implementation of Secure Flight.

Improved and standardized technology

TSA leveraged existing systems and used "industry-standard commercial-off-the-shelf" (COTS) software in developing the Secure Flight DSS.[166] Former TSA Deputy Administrator Gail Rossides said the end product was an "efficient, cost-effective, and responsive system," and credited the data submission process with being "flexible."[167] While this is not an evaluation of the appropriateness of the systems selected or the quality of the developed Secure Flight product, it is important to note technological improvements over the previous system of aircraft operators conducting their own matches. TSA suggests that the system fully "raises the baseline standard in terms of the technology and automation,"[168] and arguably it does. By integrating all watch list matching under Secure Flight system, at a very minimum, baselines and standards in information security and the use of automation technology are established.[169] Centralizing watch list matching also permits technological improvements to be applied

[163] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Communications Toolkit: Talking Points for Editorial from TSA." July 20, 2010, Version 3.0. http://www.tsa.gov/content/communications-toolkit.

[164] United Airlines. "Secure Flight." http://www.united.com/web/en-US/content/travel/airport/id/secure.aspx. (Accessed May 21, 2014).

[165] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=172. (Accessed May 26, 2014).

[166] The Secure Flight program's two operations centers run identical configurations of hardware and commercial off-the-shelf software. Key components include IBM's DB2 relational database, the IBM Tivoli product suite, IBM Websphere MQ series messaging backbone, and IBM Rational ClearCase software management running on UNIX/AIX and Windows operating systems.

[167] Patrick Marshall. "Secure Flight's off-the-shelf recipe." *GCN*. http://gcn.com/articles/2011/10/17/tsa-secure-flight-tech-sidebar.aspx. (Accessed May 11, 2014).

[168] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Communications Toolkit: Talking Points for Editorial from TSA." July 20, 2010, Version 3.0. http://www.tsa.gov/content/communications-toolkit.

[169] Patrick Marshall. "Secure Flight's off-the-shelf recipe." *GCN*. http://gcn.com/articles/2011/10/17/tsa-secure-flight-tech-sidebar.aspx. (Accessed May 11, 2014).

systemically. One might argue that private industry could deploy system upgrades more nimbly than the federal government. However, compelling airlines to continuously upgrade their systems would likely require regulations and incentives. The TSA has the organizational mission to "provide the most effective transportation security in the most efficient way"[170] and can be expected to fund, develop, and deploy improvements to Secure Flight technology.

Watch list distribution

When matching was conducted by individual airlines, static versions of the terror watch lists were being distributed.[171] There were limited controls on what happened to those lists after they left the possession of the U.S. Government.[172] Though this is not a benefit of automation specifically, the program itself results in a benefit to national security by limiting the distribution of sensitive watch list data, decreasing the risk of the lists being compromised.[173] Furthermore, information security risks are more difficult to manage in distributed systems than in closed systems.[174] Keeping PII and national security information within a closed system with access controls enhances both security and privacy. Access controls on closed systems also provide mechanisms for deterring internal abuse, often referred to as "insider threats."

Ability to utilize risk-based security procedures

In addition to more effectively identifying individuals on the No Fly and Selectee Lists and coordinating appropriate responses to matches, the implementation of Secure

---

[170] U.S. Department of Homeland Security, Transportation Security Administration. "Mission, Vision, and Core Values." January, 2014. http://www.tsa.gov/about-tsa/mission-vision-and-core-values. (Accessed May 26, 2014).

[171] U.S. Department of Homeland Security. *Advance Passenger Information System Pre-Departure Final Rule & Secure Flight Notice of Rule Making.* (Washington, DC: Department of Homeland Security, n.d.). http://www.hlswatch.com/sitedocs/apis-secure-flight-joint-faqs.pdf.

[172] U.S. Department of Homeland Security Transportation Security Administration. "Secure Flight: Your safety is our priority." Presentation to GBTA Conference, April 22, 2009. http://www.gbta.org/Lists/Resource%20Library/NBTAWebinar_SecureFlight.pdf .

[173] United Airlines. "Secure Flight." http://www.united.com/web/en-US/content/travel/airport/id/secure.aspx. (Accessed May 21, 2014).

[174] Tom Welsh. "The Security Risks of Modern Distributed Systems." *CSO Online*. November 9, 2005. http://www.csoonline.com/article/2119090/data-protection/the-security-risks-of-modern-distributed-systems.html. (Accessed July 11, 2014).

Flight supports risk-based security procedures. TSA's Risk-Based Security (RBS) mission is to "focus its resources and improve the passenger experience at security checkpoints."[175] TSA is now using its Secure Flight system to identify travelers who may be eligible for expedited screening by using information already collected and provided to TSA by the airlines.[176] Moving passengers who are identified as "low-risk" to an expedited screening queue allows TSA to focus its screening efforts on passengers who are more likely to pose a threat.[177] Incorporating this type of risk-based assessment in security procedures may preserve or improve national security in the face of a growing traveling population[178] and relatively stagnant resources and budgets.

Statistics on resource reduction from this effort are not available. A 2011 analysis published by the National Security Research Division at RAND showed that simultaneous resource and risk-reduction are possible with the incorporation of risk-based security screenings such as using passenger data or trusted traveler programs to expedite the screening of certain passengers.[179] However, random selection for expedited screening at airports is raising public concern over privacy.[180] Though passengers benefit from the expedited screening procedures, they do not know why or how they were selected. Publishing these criteria might make it easier for terrorists or other criminals to exploit the system. Public education that does not compromise the process could mitigate privacy concerns.

---

[175] White House, Federal IT Dashboard. "Transportation Security Administration: Secure Flight." https://itdashboard.gov/investment?buscid=172. (Accessed May 26, 2014).

[176] U.S. Department of Homeland Security, Transportation Security Administration. "Risk-Based Security Initiatives." February 10, 2014. http://www.tsa.gov/traveler-information/tsa-risk-assessments. (Accessed May 26, 2014).

[177] U.S. Department of Homeland Security, Office of Privacy. "Privacy Impact Assessment Update for Secure Flight DHS/TSA/PIA - 018(e)." April 13, 2012. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight_update018%28e%29.pdf.

[178] U.S. Department of Homeland Security, Transportation Security Administration. "Secure Flight Overview." March 19, 2014, http://www.tsa.gov/stakeholders/secure-flight-program.

[179] Brian A. Jackson, Edward W. Chan, and Tom LaTourrette. "Assessing the Security Benefits of a Trusted Traveler Program in the Presence of Attempted Attacker Exploitation and Compromise." (Santa Monica, CA: Rand Corp., May 2011). http://www.rand.org/content/dam/rand/pubs/working_papers/2011/RAND_WR855.pdf. (Accessed July 11, 2014).

[180] Amar Toor. "PreCheck unchecked: why the TSA is putting more people in the fast lane." *The Verge*. January 14, 2014. http://www.theverge.com/2014/1/14/5307000/why-is-the-tsa-pushing-everyone-through-precheck-security-screening. (Accessed July 11, 2014).

b. Risks to National Security

False identities and documents

Often cited as a weakness of passenger watch list matching are challenges with identify verification and false document use. Secure Flight would likely identify a terrorist who willingly offered an airline his/her real name, true age and gender, and valid passport or other identification documents. However, someone attempting to defeat Secure Flight or any other matching system might make the effort to use a false identity and false documents. TSA investigated the possibility of using commercially available data to verify information that was being processed by Secure Flight, potentially mitigating some of this risk. TSA had intended to use information such as driving records and credit history to verify the accuracy of information provided by travelers.[181] Criticism of the privacy impacts of the use of commercial data prompted TSA to discontinue testing and abandon the inclusion of commercial data in Secure Flight.[182]

Though Secure Flight does not offer an improvement validating the identity and documents provided by a passenger, the use of Secure Flight's automation tools for watch list matching is no worse than the previous systems.

4. Findings

The fundamental factors for evaluating the policy decision to implement automation tools for immigration adjudication procedures as outlined in the methodology for this analysis are:

- expected benefits to stakeholders,
- potential improvements in operational efficiency, and
- potential reduction of risks to national security.

[181] Ronald London. "Secure Flight Will Not Use Commercial Databases." Privacy Security Law Blog. http://www.privsecblog.com/2005/09/articles/policy-regulatory-positioning/secure-flight-will-not-use-commercial-databases/. (Accessed July 19, 2014).

[182] EPIC - Electronic Privacy Information Center. "Secure Flight." EPIC. http://www.epic.org/privacy/airtravel/secureflight.html. (Accessed July 19, 2014).

The previous analysis shows that these factors are *substantially demonstrated* by the Secure Flight program. This case study thus supports the development and implementation of automation tools for immigration adjudications.

III. AUTOMATED CONTINUOUS EVALUATION SYSTEM (ACES) CASE STUDY

A. OVERVIEW

The United States Congress targeted longstanding problems with the timeliness and coordination of procedures for investigating and adjudicating national security clearances with mandates in the Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA).[183] Through the IRTPA, Congress challenged federal government agencies to improve processing of security clearances, including evaluating the use of "available information technology and databases" to expedite investigative and adjudicative procedures and to "verify standard information submitted as part of an application for a security clearance."[184] The Automated Continuous Evaluation System (ACES), developed by the Defense Personnel and Security Research Center (PERSEREC), is a decision support system (DSS) that can be used to automate certain procedures to accelerate the processing of security clearance eligibility determinations.[185]

1. Program Mission

Inefficiencies in the federal personnel security system have been the target of reformers for decades. The attacks of September 11, 2001 highlighted these inefficiencies and brought attention to the need for reform. The terror attack produced a "flood of additional security clearance requests"[186] that threatened to overwhelm the personnel security system by adding to the backlog of overdue clearance decisions. Congress

---

[183] Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA), Pub. L. No. 108–458, 118 Stat. 3638 (Dec. 17, 2004), codified at 42 U.S.C. §2000ee, 50 U.S.C. §403-1 et seq., §403-3 et seq., §404o et. seq.

[184] Ibid.

[185] Erik L. Lang. *Adjudication Decision Support (ADS) System Automated Approval Estimates for NACLC Investigations*. Technical Report 07–04. (Monterey, CA: Defense Personnel Security Research Center (PERSEREC), May 2007). http://www.dhra.mil/perserec/reports/tr07-04.pdf.

[186] Leissa C. Nelson and Samantha A. Smith-Pritchard. *Baseline Suitability Analysis*. Technical Report 13–05. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), July 2013). https://www.hsdl.org/?view&did=751526.

responded by passing the Intelligence Reform and Terrorism Prevention Act (IRTPA)[187] in December 2004. IRTPA set aggressive mandates for improving procedures for granting security clearances including specific timelines for completing background investigations and adjudications. At that time, there was a tremendous national backlog of pending security clearance determinations.[188] Additionally, in 2005, the Government Accountability Office (GAO), which had been critical of the security clearance process for years, placed the Department of Defense's personnel security system on its "High Risk List."[189] Programs on this list are monitored closely until improvements satisfy GAO evaluators.

These two factors prompted earnest efforts to reform the personnel security system across the federal government. In June 2007, the Joint Security Process Reform Team was formed by a memorandum of agreement between the Department of Defense (DOD) and the Office of the Director of National Intelligence (ODNI).[190] Issued in June 2008, Presidential Executive Order 13467[191] expanded the Joint Security Process Reform Team to include the Office of Management and Budget (OMB) and the Office of Personnel Management (OPM) and established the Performance Accountability Council (PAC). The PAC, comprised of representatives of all the aforementioned executive

---

[187] Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA). Pub. L. No. 108–458, 118 Stat. 3638 (Dec. 17, 2004), *codified at* 42 U.S.C. §2000ee, 50 U.S.C. §403-1 *et seq.*, §403-3 *et seq.*, §404o *et. seq.*

[188] Kathy L. Dillaman. Associate Director For Federal Investigative Services, Office of Personnel Management. *Personnel Security Clearance Reform.* Statement before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, United States House of Representatives. December 1, 2010. http://www.opm.gov/news/testimony/111th-congress/personnel-security-clearance-reform/.

[189] U.S. Government Accountability Office. *High-Risk Series: An Update.* (GAO-05-207) (Washington, DC: GPO, 2005). http://www.gao.gov/products/GAO-05-207.

[190] U.S. Government Accountability Office. *Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum*. (GAO-11-65) (Washington, DC: GPO, 2011). http://www.gao.gov/products/GAO-11-65.

[191] Executive Order no. 13467 of June 30, 2008, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information. *Code of Federal Regulations*, title 3, part 13467, (2008). http://www.ncix.gov/publications/policy/docs/EO_13467.pdf.

agencies and chaired by the Deputy Director for Management, OMB, is accountable to the President and drives reform efforts and oversees their implementation.[192]

The Executive Order requested a reform proposal to make hiring and clearing decisions more quickly, effectively, and efficiently, and to achieve the mandates of IRTPA.[193] These mandates are:

- Ensure that background investigations and clearance determinations completed by an authorized investigative agency or authorized adjudicative agency are transferable and accepted by all other agencies with equivalent or lesser requirements.

- Establish and operate an integrated, secure database for storing information relevant to the granting, denial or revocation of security or suitability clearances from all authorized agencies.

- Evaluate and leverage information technology and databases to expedite investigative and adjudicative processes.

- Meet specific timeliness goals, such as making end-to-end determinations on 90% of clearance requests within an average of 60 days.[194]

The names used to refer to the conglomeration of agencies and the program to reform security and suitability processes have evolved. The "Joint Security Process Reform Team," then later the "The Joint Suitability and Security Clearance Reform Effort," is now generally referred to as the "Joint Reform Effort" or "JRE." The leadership of the Executive Branch entities involved in the program is now called the "Performance Accountability Council" (PAC). This analysis will refer to the program of reform as the "JRE" and the team of leaders as the "PAC."

---

[192] Security and Suitability Performance Accountability Council (PAC). *Security and Suitability Process Reform Strategic Framework*. (Washington, DC: Security and Sustainability Performance Accountability Council, February 2010). http://www.nationalsecuritylaw.org/files/received/OMB/Security_and_Suitability_Process_Reform-Strategic_Framework.pdf.

[193] Leissa C. Nelson and Samantha A. Smith-Pritchard. *Baseline Suitability Analysis*. Technical Report 13–05. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), July 2013). https://www.hsdl.org/?view&did=751526.

[194] Security and Suitability Performance Accountability Council (PAC), *Security and Suitability Process Reform Strategic Framework*. (Washington, DC: Security and Sustainability Performance Accountability Council, February 2010). http://www.nationalsecuritylaw.org/files/received/OMB/Security_and_Suitability_Process_Reform-Strategic_Framework.pdf.

2. Background

Security and Suitability Clearances

A "security clearance" is a determination that an individual—whether a direct federal employee or a private contractor performing work for the government—is eligible for access to classified national security information. A background investigation and adjudication process is conducted for candidates for security clearances in an effort to ensure that classified information is entrusted only to those "who have proven reliability and loyalty to the nation"[195] because its disclosure may have the potential to cause grave damage to national security if disclosed. In addition to the appropriate level of clearance, an individual must also have a demonstrated "need to know" the information contained in classified materials for their job duties.[196]

There are three general levels of security clearances. They correspond to the levels of sensitivity of the information that a cleared individual is eligible to access: Confidential, Secret, and Top Secret (TS). In addition, individuals with TS level clearance may be approved for access to particularly vulnerable information categorized as Sensitive Compartmented Information (TS/SCI) and/or Special Access Programs (SAP).[197]

"Suitability" refers to a determination that individuals seeking employment with the United States federal government will "perform their duties with integrity and promote the common good of the public and the agency they serve."[198] This determination also requires an investigation and adjudication. Clearance and suitability determinations remain valid for a specified number of years after the completion of the

---

[195] U.S. Government Accountability Office. *Personnel Security Clearances: An Outcome-Focused Strategy Is Needed to Guide Implementation of the Reformed Clearance Process.* (GAO-09-488) (Washington, DC: GPO, 2009). http://www.gao.gov/products/GAO-09-488 .

[196] Michelle D. Christensen and Frederick M. Kaiser, *Security Clearance Process: Answers to Frequently Asked Questions*, (CRS Report RL R43216) (Washington, DC: Office of Congressional Research Service, September 9, 2013). http://fas.org/sgp/crs/secrecy/R43216.pdf.

[197] Ibid.

[198] Leissa C. Nelson and Samantha A. Smith-Pritchard. *Baseline Suitability Analysis*. Technical Report 13–05. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), July 2013). https://www.hsdl.org/?view&did=751526.

investigation; then, periodic reinvestigations are required. Periodic reinvestigation cycles differ by level of clearance. For example, an individual holding a Secret clearance must be reinvestigated at least once every 10 years; an individual holding a Top Secret Clearance must be reinvestigated at least once every 5 years."[199] Nearly 5 million federal employees and contractors hold Secret or Top Secret security clearances.[200]

Investigation and adjudication requirements and processes

There are different levels of investigation. Eligibility standards and investigative requirements depend on the clearance level being sought for a prospective employee.[201] The specific standards and requirements for a clearance level or suitability determination are national security information, and thus are classified. As an example, the investigation for a TS/SCI clearance might involve a polygraph test while an investigation for a Secret clearance likely would not.

On August 29, 2011, the Office of Personnel Management (OPM) published revised National Investigative Standards. The "Federal Investigations Notice" announced full implementation of updated procedures in an effort to align clearance levels and investigative requirements across the federal government, facilitating reciprocity, as required by IRTPA. The updated procedures were initially agreed upon by OPM and ODNI on August 24, 2010, and fully implemented October 1, 2011.[202] Table 1

---

[199] U.S. Government Accountability Office. *More Accurate Estimate of Overdue Security Clearance Reinvestigations is Needed*. (GAO/T-NSIAD-00-246) (Washington, DC: GPO, 2000). http://gao.gov/assets/110/108657.pdf. Also see: U.S. Government Accountability Office. *Personnel Security Clearances: Continuing Leadership and Attention Can Enhance Momentum Gained from Reform Effort*. (GAO-12-815T) (Washington, DC: GPO, 2012). http://gao.gov/assets/600/591784.pdf.

[200] Peter Eisler and Tom Vanden Brook. "Security clearances: Holes in the system?" *USA Today*. September 30, 2013. http://www.usatoday.com/story/news/nation/2013/09/30/problems-with-security-clearances/2897303/. (Accessed July 5, 2014). See also Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

[201] Michelle D. Christensen and Frederick M. Kaiser, *Security Clearance Process: Answers to Frequently Asked Questions*. (CRS Report RL R43216) (Washington, DC: Office of Congressional Research Service, September 9, 2013). http://fas.org/sgp/crs/secrecy/R43216.pdf.

[202] United States Office of Personnel Management, Federal Investigative Services. "Continuous Efforts to Align with Reciprocity Goals and Timeliness Standards." Federal Investigations Notice 11–04. August 29, 2011. http://www.opm.gov/investigations/background-investigations/federal-investigations-notices/2011/fin11-04.pdf.

demonstrates how the investigative requirements increase with a higher level of clearance:

LEVEL	POSITION	FORM	INVESTIGATION	REINVESTIGATION
Tier 1	Low Risk Non-sensitive, including HSPD-12 Credentialing	SF85	NACI	None
Tier 2a	Low Risk Non-critical sensitive, including Confidential, Secret, & L access eligibility for contractors & military	SF86	NACLC	NACLC every 10 years
Tier 2b	Low Risk Non-critical Sensitive, including Confidential, Secret, & L access eligibility for federal employees	SF86	ANICI	NACLC every 10 years
Tier 3a	Moderate Risk PT Non-sensitive	SF85P	MBI	NACLC every 5 years
Tier 3b	Moderate Risk PT Non-critical Sensitive, including Confidential, Secret, & L access eligibility	SF86	MBI	NACLC every 5 years
Tier 4a	High Risk PT Non-sensitive	SF85P	BI	PRI every 5 years
Tier 4b	High Risk PT Non-critical Sensitive, including Confidential, Secret, & L access eligibility	SF86	BI	PRI every 5 years
Tier 5	Any risk level Critical Sensitive or Special Sensitive, including Top Secret, SCI, and Q access eligibility	SF86	SSBI	SSBI-PR or PPR every 5 years

Table 1. Tiered Investigative Model (after OPM, 2011)[203]

Both personnel security and suitability investigation processes rely on similar background data, but historically the processes and determinations have not been well coordinated, nor have results or data been shared to facilitate employment movement between agencies or even positions within agencies.[204] Executive Order 13467[205]

[203] United States Office of Personnel Management, Federal Investigative Services. "Continuous Efforts to Align with Reciprocity Goals and Timeliness Standards." Federal Investigations Notice 11–04. August 29, 2011. http://www.opm.gov/investigations/background-investigations/federal-investigations-notices/2011/fin11-04.pdf.

[204] Leissa C. Nelson and Samantha A. Smith-Pritchard. *Baseline Suitability Analysis*. Technical Report 13–05. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC). July 2013). https://www.hsdl.org/?view&did=751526.

included a request to bring these processes into better alignment, and the PAC committed to this goal in the 2010 Strategic Framework. Because of their similarities, the investigative and adjudicative processes for security clearances and suitability will be referenced as the "clearance process." For analytical purposes of this thesis, the steps in these processes that could be supported with automation or decision support tools are generally the same.

The clearance process involves a number of stages. The key steps are request, investigation, adjudication, and reinvestigation.

- *Request*. During this phase, a sponsoring agency determines that an employee or contractor requires an investigation. For a security clearance, an individual will submit all information required on the Standard Form 86 (SF-86). For a suitability determination, an individual submits all required information on the Standard Form 85P (SF-85P).[206]

- *Investigation*. Using the information provided by the applicant in his or her clearance application materials, a background investigation of the applicant is conducted. The background investigation may vary in terms of content, cost, and length of time for completion depending, in part, on the level of clearance being sought.[207]

- *Adjudication*. During the adjudication phase, the sponsoring agency uses information obtained in the investigation to decide whether to grant a security clearance or favorable suitability determination.

- *Reinvestigation*. Individuals are subject to periodic reinvestigations to maintain clearances. The frequency of reinvestigations varies by level of clearance and may vary across agencies.

Figure 6 demonstrates the basic phases of the process for an initial clearance or suitability determination.

---

[205] Executive Order no. 13467 of June 30, 2008, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information. *Code of Federal Regulations*, title 3, part 13467, (2008). http://www.ncix.gov/publications/policy/docs/EO_13467.pdf.

[206] Federal government positions covered by 5, Code of Federal Regulations, part 731 (5 CFR 731) are those in the competitive service, those in the excepted service where the incumbent can be noncompetitively converted to the competitive service, or a career appointment to the Senior Executive Service. Investigative requirements are described at 5 CFR 731.104. Under 5 CFR 731.

[207] Michelle D. Christensen and Frederick M. Kaiser, *Security Clearance Process: Answers to Frequently Asked Questions*. (CRS Report RL R43216) (Washington, DC: Office of Congressional Research Service, September 9, 2013). http://fas.org/sgp/crs/secrecy/R43216.pdf.

Figure 6. Initial Security Clearance or Suitability Investigation (from USA Today, 2013)[208]

3. Accomplishments and Plans

Since its inception in 2007, the JRE has implemented several changes in the clearance process to meet the goals of the IRTPA. A Security and Suitability Strategic Framework, published in February 2010,[209] has been guiding activities of the PAC and its member agencies. The Strategic Framework outlined overarching reform goals.

Many of the goals outlined in the Strategic Framework related directly to the mandates of IRTPA, such as Goal 1: Reciprocity, Goal 2: Development of an Integrated Database, and Goal 4: Timeliness. The Framework also identified process alignment and quality as goals 5 and 7, respectively.

According to IRTPA, "leveraging information technology" has been a major strategy for improving the clearance process. Even before the IRTPA, The 9/11 Commission Report recommended that the federal government "evaluate the use of available information technology and databases to expedite investigative and adjudicative processes for all and to verify standard information submitted as part of an application for

[208] Peter Eisler and Tom Vanden Brook. "Security clearances: Holes in the system?" USA Today. September 30, 2013. http://www.usatoday.com/story/news/nation/2013/09/30/problems-with-security-clearances/2897303/ . (Accessed July 5, 2014).

[209] Security and Suitability Performance Accountability Council (PAC). *Security and Suitability Process Reform Strategic Framework*. (Washington, DC: Security and Sustainability Performance Accountability Council, February 2010). http://www.nationalsecuritylaw.org/files/received/OMB/Security_and_Suitability_Process_Reform-Strategic_Framework.pdf.

a security clearance."[210] With the publication of the Strategic Framework, the use of automation tools became an explicit goal for reform. Goal 3 identifies "IT/End-to-End Automation" and Goal 6 is "Continuous Evaluation."[211]

The PAC set out to achieve these goals with a vision for seven identified phases of processing. Figure 7 depicts the seven phases:

Figure 7. Security and Suitability Reform Strategic Framework (from JRE, 2008)[212]

In its vision for a reformed system, the JRE specified procedures for using automation decision support tools and modified investigative procedures. The JRE identified "automated records checks" (ARC) that it envisioned would "provide an automated process to run subject data against appropriate government and validated commercial databases to collect, analyze, and validate data."[213] It further specified a "case flagging strategy," such that any issues discovered during ARC would trigger an "Expandable Focused Investigation" (EFI). As opposed to the previous approach of routinely pursuing all information in a case, EFI was intended to focus investigative field resources only on those potential issues discovered through ARC. This focused approach was expected to result in process efficiency and improved timelines. The revised investigative standards published in 2011 mandated an EFI at all tiers when issue cases

[210] Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA). Pub. L. No. 108–458, 118 Stat. 3638 (Dec. 17, 2004), *codified at* 42 U.S.C. §2000ee, 50 U.S.C. §403-1 *et seq.*, §403-3 *et seq.*, §404o *et. seq.*

[211] Security and Suitability Performance Accountability Council (PAC). *Security and Suitability Process Reform Strategic Framework*. (Washington, DC: Security and Sustainability Performance Accountability Council, February 2010). http://www.nationalsecuritylaw.org/files/received/OMB/Security_and_Suitability_Process_Reform-Strategic_Framework.pdf.

[212] Ibid.

[213] Ibid.

are flagged. The JRE expected this combined strategy to provide "cost, consistency, and time efficiencies."[214]

In addition to using ARC for initial clearance investigations, the JRE planned to more frequently evaluate personnel who have access to classified information with improved Continuous Evaluation (CE) processes and standards. The vision for CE has been to keep the process streamlined, utilizing EFI only if issues were discovered during ARC.

4. Continuous Improvement

Significant overall progress has been made to improve the investigation and adjudication of personnel security clearance applications in a timely manner. The GAO reported in 2010 that the "majority of clearances" are processed within the IRTPA established goal of 60 days. At that time, certain agencies continued to face challenges in meeting timeliness objectives.[215]

The Office of Personnel Management, Federal Investigative Services (OPM-FIS) OPM, which conducts approximately 95 percent of the total background investigations government-wide,[216] cites "program efficiencies and expanded use of technology" as keys to achieving and sustaining timeline goals.[217] As part of the reform process and as recommended by the 9/11 Commission that a "single federal agency"[218] be responsible

---

[214] Security and Suitability Performance Accountability Council (PAC). *Security and Suitability Process Reform Strategic Framework.* (Washington, DC: Security and Sustainability Performance Accountability Council, February 2010). http://www.nationalsecuritylaw.org/files/received/OMB/Security_and_Suitability_Process_Reform-Strategic_Framework.pdf .

[215] U.S. Government Accountability Office. *Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum.* (GAO-11-65) (Washington, DC: GPO, 2010). http://www.gao.gov/products/GAO-11-65.

[216] Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

[217] Kathy L. Dillaman. Associate Director For Federal Investigative Services, Office of Personnel Management. *Personnel Security Clearance Reform.* Statement before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, United States House of Representatives. December 1, 2010. http://www.opm.gov/news/testimony/111th-congress/personnel-security-clearance-reform/.

[218] National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report* (New York: W.W. Norton & Co., 2004).

for clearance processing, most clearance investigations have been brought under OPM-FIS.

Recent events involving individuals holding security clearances have raised concerns about "missed red flags" in background investigations.[219] The tragic event at the Washington Navy Yard, where 34-year-old IT contractor Aaron Alexis opened fire and killed 12 people, as well as the disclosure of classified information by National Security Agency (NSA) contractor Edward Snowden, have drawn public attention to the clearance process.

Efforts to improve the timeliness, efficiency, and quality of the clearance process have proven challenging, and the GAO continues to identify opportunities for continuous improvement.[220] In February 2014, the White House released an interagency review of the federal security clearance process.[221] Two priorities recommended in the report include implementing continuous evaluation (CE) improvements and improving access to relevant information, especially state and local law enforcement records.[222] The JRE's vision for CE in the reformed process includes the implementation of automated records checks of commercial databases, government databases, and other information lawfully available.[223]

---

[219] Jack Moore. Federal News Radio Online. "White House backs 13 recommendations to improve security clearance process." March 19 2014. http://www.federalnewsradio.com/520/3585372/White-House-backs-13-recommendations-to-improve-security-clearance-process .

[220] U.S. Government Accountability Office. *Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum*. (GAO-11-65) (Washington, DC: GPO, 2010). http://www.gao.gov/products/GAO-11-65.

[221] Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

[222] Jack Moore. Federal News Radio Online. "White House backs 13 recommendations to improve security clearance process." March 19 2014. http://www.federalnewsradio.com/520/3585372/White-House-backs-13-recommendations-to-improve-security-clearance-process.

[223] Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

B. USE OF AUTOMATION AND DECISION-SUPPORT SYSTEMS

The Security and Suitability Process Reform Strategic Framework released in February 2010 specified the evaluation and piloting of a system developed by Defense Personnel Security Research Center (PERSEREC) called the Automated Continuous Evaluation System (ACES) in several ARC and CE applications, such as:

- integrate ACES records checks into an ARC product line for the Office of Personnel Management (OPM),
- pilot ARC capability for processing government and commercial databases,
- evaluate ARC capability for enabling the "flagging strategy" and EFI,
- pilot ACES at the National Reconnaissance Office (NRO) and State Department,
- validate ARC for annual CE for individuals cleared at TS/SCI, and
- pilot ACES CE Capability within DOD.[224]

JRE member agency DOD had invested in research into automated records checks since 1999 when it requested that PERSEREC plan a prototype.[225] In 2008, the JRE identified ACES for inclusion in the reformed federal security clearance process,[226] and the direction of ACES research and development shifted to reflect the goals of the JRE and the emerging national program.[227]

---

[224] Security and Suitability Performance Accountability Council (PAC). *Security and Suitability Process Reform Strategic Framework*. (Washington, DC: Security and Sustainability Performance Accountability Council, February 2010). http://www.nationalsecuritylaw.org/files/received/OMB/Security_and_Suitability_Process_Reform-Strategic_Framework.pdf .

[225] Eric L. Lang. *The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security*. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), September 2013).

[226] Ibid.

[227] Eric L. Lang. *The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security*. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), September 2013).

Automated Continuous Evaluation System (ACES)

The Defense Personnel and Security Research Center (PERSEREC) developed the Automated Continuous Evaluation System (ACES). ACES is an automated system that can check an applicant against 40 government and commercial databases. It uses an applicant's personally identifiable information (PII) or responses provided on the Standard Form 86 (SF-86) or Standard Form 85P (SF-85P) against these data sources to locate potentially adverse information, verify what has been submitted, and collect more information in those systems. It applies business rules to data and produces a report that flags issues of potential security concern. The report is then transmitted to an approved adjudicator or facility.[228]

Since its beginnings in the late 1990s, ACES has evolved through iterations of research and beta testing which began in 2005.[229] When it was identified for use in ARC by the JRE in 2009, researchers began several pilot studies to demonstrate ACES' capabilities for various federal agencies with different types of investigations.[230] According to developers, these pilot projects demonstrated that ACES can "streamline the expensive security clearance and suitability vetting process" and reduce processing costs.[231] Research validated the use of ARC to flag issues up front, allowing field investigative resources to focus on cases with issues.[232]

ARC

Automated records checks have been implemented at the Office of Personnel Management. In her testimony before the 111th Congress in 2010, Associate Director for OPM Federal Investigative Services (OPM-FIS) Kathy L. Dillaman stated that

---

[228] Ibid.

[229] Defense Personnel and Security Research Center (PERSEREC). "Past Achievements." http://www.dhra.mil/perserec/pastachievements.html#ACES_2014. (Accessed July 5, 2014).

[230] Eric L. Lang. *The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security*. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), September 2013).

[231] Ibid.

[232] Joint Security and Suitability Reform Team. "Security and Suitability Process Reform." December 2008. http://www.whitehouse.gov/sites/default/files/omb/assets/omb/reports/joint_security_dec2008.pdf.

"investigations to support a Secret level security clearance include automated and manual checks of criminal history, terrorist activities, credit, and foreign activities and influence. When the checks identify issues of concern, additional checks, including interviews and other more manual efforts, are conducted as needed."[233] The conversion from manual to automated records checks has allowed OPM to "use its investigative resources more effectively" and to "reduce costs and processing time." Currently, it takes OPM an average of three days to complete these automated record checks.[234]

EFI

Implementation of EFI fell behind the initial schedule to be operational by September 2010. The most recent available information suggests that full implementation was intended for December 2013.[235] However, the 2014 report to the White House suggested that EFI has been at least partially implemented. The report suggests that security clearance include "automated and manual checks of criminal history, terrorist activities, credit, and foreign activities and influence" and that "additional checks, including interviews and other more manual efforts" proceed when initial checks reveal issues of concern.[236]

CE

As previously noted CE has not yet been fully implemented. Several pilot studies have been conducted to demonstrate ACES capabilities, including a test of 3,370 Army service members, civilian employees, and contractor personnel. This study identified

---

[233] Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

[234] Kathy L. Dillaman, Associate Director For Federal Investigative Services, Office of Personnel Management. *Personnel Security Clearance Reform.* Statement before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, United States House of Representatives. December 1, 2010. http://www.opm.gov/news/testimony/111th-congress/personnel-security-clearance-reform/.

[235] William Henderson. "Federal Suitability and Security Clearance Reform Defense News." September 21, 2010). http://news.clearancejobs.com/2010/09/21/federal-security-and-suitability-process-reform/. (Accessed July 25, 2014).

[236] Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

previously unreported derogatory information for 21.7 percent of the tested population that had developed since the last investigation. Serious derogatory information that resulted in a revocation or suspension of a security clearance was identified for 3 percent of that population.[237] The testimony of OPM-FIS Associate Director Dillaman seems to suggest that CE is at least partially implemented at that agency. Dillaman refers to an "investigation product" utilizing automated records checks for annual assessments of individuals with TS clearance.[238]

1. Development Status and System Performance

Automated records checks using the ACES tool are partially implemented in the security clearance process. Expanding the use of automation and decision support tools for clearance processing is being piloted and tested in several instances throughout the federal government. The federal government has benefited from the fact that automation research was well underway at the time the JRE prioritized its implementation. Given the success of the pilots, it is likely that agencies will leverage proven, existing tools like ACES rather than build others. Implementing ARC for both initial investigations and CE is a significant step towards the JRE's goal of end-to-end automation.

The performance of ARC in the clearance process is being demonstrated at OPM, which provides background investigations for over 100 federal agencies. OPM-FIS now utilizes automated systems with "demonstrated ample capacity to efficiently handle this demanding workload."[239]

---

[237] Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

[238] Kathy L. Dillaman, Associate Director For Federal Investigative Services, Office of Personnel Management. *Personnel Security Clearance Reform.* Statement before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, United States House of Representatives. December 1, 2010. http://www.opm.gov/news/testimony/111th-congress/personnel-security-clearance-reform/.

[239] Kathy L. Dillaman. Associate Director For Federal Investigative Services, Office of Personnel Management. *Personnel Security Clearance Reform.* Statement before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, United States House of Representatives. December 1, 2010. http://www.opm.gov/news/testimony/111th-congress/personnel-security-clearance-reform/.

Pilot projects and tests of the ACES system are underway that incorporate automated credit checks, personnel records and even social media screenings. For example, the Defense Department recently sampled more than 3,300 Army service members, civilian employees and contractors using its Automated Continuous Evaluation System (ACES). That review turned up previously unreported derogatory information on more than 21 percent of the employees sampled and serious issues, such as domestic abuse or drug abuse, in 3 percent of the clearance holders surveyed."[240]

C. ANALYSIS

The use of DSS to automate records checks for individuals who are being examined for a security clearance by automatically clearing those with no derogatory information or flagging and referring those that have issues for in-depth review offers several benefits to stakeholders. These include improvements to processing times, national security benefits through risk reduction, and direct operational efficiencies to the agencies responsible for processing clearances. Costs for this model are generally related to systems development.

1. Benefits and Costs to Stakeholders

a. Benefits to Federal Agencies

Federal agencies and contractors sponsoring a candidate for a security clearance are the primary beneficiaries of DSS for security clearance investigations and adjudications. There are interrelated national security benefits to the efficient automated processing of security clearances, such as ensuring the integrity of the work performed at these agencies and securing their classified information. National security benefits related to the implementation of automation in security clearance processing will be examined separately in a later section.

Typically, the requesting agency pays for background investigations of federal employees and contractor employees. As stated above, the vast majority of federal

[240] Jack Moore. Federal News Radio Online. "White House Backs 13 Recommendations to Improve Security Clearance process." March 19 2014. http://www.federalnewsradio.com/520/3585372/White-House-backs-13-recommendations-to-improve-security-clearance-process

background investigations (over 90%) are handled by OPM-FIS, which charges other federal agencies for the investigations it oversees.[241] The cost of background investigations vary depending on the level of clearance requested and the scope of the investigation conducted.[242] Whether or not automation would affect these fees is unknown and relatively unlikely; however, the time saved in anticipating and adjudicating a clearance has a cost or resource savings to federal agencies and contractors.

When a federal agency makes an offer of employment to an individual, that person is not permitted to "enter on duty" (EOD) until a suitability or clearance determination is made. In some cases, a preliminary determination can be made to allow an individual to begin work, but only on activities not requiring access to classified information. In many cases, an individual must wait for a complete adjudication, and the sponsoring agency must wait as well. The agency must then operate with vacancies until the individual is cleared to EOD. This has a negative impact on the agency's productivity. For contracting companies, an individual may be employed for an extended period of time on non-billable work until an adjudication can be made. Reducing the amount of time to a final adjudication through the use of automation and DSS would benefit the productivity of the sponsoring federal agencies and the profitability of contracting firms.

b. Costs to Federal Agencies

Training costs

Personnel security offices within federal agencies may be required to learn new systems to review or retrieve results that are generated by automated systems or communicated electronically from OPM investigators. Often, access to sensitive systems

[241] A summary of the investigative products offered by OPM-FIS is available at http://www.opm.gov/investigations/background-investigations/reference/annual-report-for-fiscal-year-2012.pdf.

[242] OPM's Investigations Reimbursable Billing Rates for FY2013 are available at http://www.opm.gov/investigations/ background-investigations/federal-investigations-notices/2012/fin12-07.pdf. OPM's "Position Designation Tool," which provides agencies with guidelines for determining the type of investigation required for certain government and contractor positions, is available at http://archive.opm.gov/investigate/resources/position/Position%20Designation%20System%20October%202010.pdf.

requires federal employees to maintain current training records for continued access. These training costs may include recurring activities and resources.

c. Benefits to Individuals Being Investigated

Reduced processing time

An individual being investigated for a security or suitability clearance realizes similar benefits to those of the employing agency or contracting firm in the form of time. First, with the potential to be cleared or approved automatically, an individual may be spared the time and cost of participating in an interview. Secondly, automated steps in the adjudication process may mean that a person can begin employment more quickly. This translates directly into earnings. Multiplying the average reduction in time from implementing DSS and the average salary of different types of federal and contractor employees could provide a rough calculation of the value of this benefit. However, at this time, there are no estimates of expected reduction in time to adjudication that automation would provide.

Privacy Controls

Misuses or breaches of national security systems or systems containing PII are both a security and privacy risk. Those with access to sensitive systems are required to maintain current training in privacy laws and usually must sign "Rules of Behavior"[243] forms that indicate they are familiar with the appropriate handling of PII. Access controls on closed systems also provide mechanisms for deterring internal abuse, often referred to as "insider threats." As noted in the Privacy Impact Analysis for an ACES pilot with DHS in 2007:

> ACES user roles are highly restricted and audited. ACES employs role-based access. Access to the ACES system is granted on a "need to know" basis. PERSEREC staff and contractors with access to ACES are required to complete security and data privacy training on an annual basis. Data on ACES may only be accessed by individual user account and password. Connectivity to external networks is tightly restricted to prevent the

[243] U.S. Department of Homeland Security. *General Rules of Behavior for Users of DHS Systems and IT Resources that Access, Store, Receive, or Transmit Sensitive Information*. (Washington, DC: Department of Homeland Security, n.d.). http://www.ice.gov/doclib/sevis/pdf/behavior-rules.pdf

> authorized transfer of ACES data outside the secure ACES network enclave. System security logs are audited on a regular basis to ensure compliance with all privacy and data security requirements.[244]

Presumably, these privacy and security controls have been maintained as ACES has been expanded beyond pilots and test environments.

It is important to note that when an individual consents to a background investigation in support of an application for a security clearance, he or she must sign an "Authorization for Release of Information."[245] An individual has the right to decline to provide his or her personal information, but doing so means the individual cannot be granted a security clearance. Furthermore, under Executive Order 12968, "Access to Classified Information," all employees are subject to investigation by an appropriate government authority "prior to and at any time during the period of access to determine whether they continue to meet the requirements for access." Individuals undergoing background investigations have due process rights under Section 5.2 of Executive Order 12968, including the opportunity to correct errors, provide mitigating information, or appeal a negative adjudication.[246]

ACES checks are only conducted on people who have signed an Authorization for Release of Information that is still valid at the time the record checks are performed. Signing the release and both seeking and maintaining national security clearances are voluntary acts. As specified in the DHS PIA, "ACES does not change these requirements and merely automates the searches."[247]

---

[244] U.S. Department of Homeland Security, Office of Privacy. "Privacy Impact Assessment for the Automated Continuing Evaluation System (ACES) Pilot." (Washington, DC: Department of Homeland Security, April 9, 2007). https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_aces.pdf

[245] See U.S. Office of Personnel Management, "Questionnaire for National Security Positions," Standard Form 86, 5 CFR Parts 731, 732, and 738. Revised December 2010. http://www.opm.gov/forms/pdf_fill/SF86.pdf

[246] Executive Order 12968 of August 4, 1995. "Access to Classified Information." *Code of Federal Regulations*, title 3, part 12968, (1995). http://www.ncix.gov/publications/policy/docs/EO_12968.pdf.

[247] U.S. Department of Homeland Security, Office of Privacy. "Privacy Impact Assessment for the Automated Continuing Evaluation System (ACES) Pilot." (Washington, DC: Department of Homeland Security, April 9, 2007). https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_aces.pdf.

d. Costs to Individuals Being Investigated

Training costs

Individuals submitting information for a security clearance or reinvestigation may be required to learn a new system to input their personal information. If the system is updated between reinvestigations, an individual may need to invest time to relearn how to enter data.

2. Benefits and Costs to Operations

a. Benefits to Operations

Cost reduction and resource alignment

PERESERC documents claim that "ACES will streamline the expensive security clearance and suitability vetting process and greatly reduce its cost."[248]Additionally, the JRE believes that the use of ARC will provide "cost and time efficiencies compared with manual investigative activities."[249] The two overarching benefits of automation support this claim. The first of these is the extent to which automated checks of systems is faster than manually checking all the systems included in ARC. OPM-FIS Associate Director for OPM Federal Investigative Services (OPM-FIS) Kathy L. Dillaman stated that ARC takes "an average of three days,"[250] but data on the duration of manual records checks was not provided. Presumably, 3 days was an improvement over the previous procedure, and thus a direct benefit to the agency.

The second benefit supporting cost reduction claims is the extent to which resources are reduced due to the use of a "case flagging strategy." The JRE

---

[248] Eric L. Lang. *The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security*. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), September 2013).

[249] Joint Security and Suitability Reform Team. *Security and Suitability Process Reform Initial Report.* April 30, 2008. http://www.whitehouse.gov/sites/default/files/omb/reports/reform_plan_report_2008.pdf.

[250] Kathy L. Dillaman. Associate Director For Federal Investigative Services, Office of Personnel Management. *Personnel Security Clearance Reform.* Statement before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, United States House of Representatives. December 1, 2010. http://www.opm.gov/news/testimony/111th-congress/personnel-security-clearance-reform/.

recommendations specifically included Automated Records Checks (ARC) and a "case flagging strategy" in the "Security and Suitability Process Reform" document submitted in December 2008.[251] The strategy entails using ARC to "identify cases requiring human investigation and adjudication" and then using electronic adjudication (eAdjudication) for "clean cases" with no flagged issues. This strategy implies that human investigations and adjudications are not utilized in the same capacity for the evaluation of all security clearances, whether initial requests or periodic reinvestigations. As of February 2014, much of this strategy has been implemented. Security clearance investigations include "automated and manual checks of criminal history, terrorist activities, credit, and foreign activities and influence."[252] When these checks identify issues of concern, "additional checks, including interviews and other more manual efforts, are conducted as needed.[253]

The JRE notes the "transition to automated case flagging" is driven by the "results of several research efforts."[254] The research showed that the flagging strategy, as described, is as effective as traditional field leads at identifying cases with issues. The case flagging strategy, in concert with Expandable Focused Investigation (EFI) methods, focuses investigative resources on the cases that need additional scrutiny. It reduces the use of human resources needed to conduct investigations and adjudications, and it results in a reduction of operational costs for the agencies responsible for processing security clearances. When known non-productive investigative activity is eliminated and investigative resources are able to appropriately focus on the issues that need them most, cost is reduced and timeliness is improved. This may also improve national security, as discussed later.

The Strategic Framework also proposed robust and expanded continuous evaluation (CE). The goal for implementing CE remains unmet as of 2014 when the

---

[251] Joint Security and Suitability Reform Team. "Security and Suitability Process Reform." December 2008 http://www.whitehouse.gov/sites/default/files/omb/assets/omb/reports/joint_security_dec2008.pdf.

[252] Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

[253] Ibid.

[254] Ibid.

Office of Management and Budget reviewed the initiative,[255] but it remains a goal of the JRE and is likely to be implemented. Expanded CE investigations would result in an increase in overall clearance workload. The use of ARC for CE in conjunction with a case flagging strategy would allow OPM to align resources and utilize human adjudicators for only those cases with flagged issues. Cost reductions and resource alignments from implementing ARC might not fully compensate for the increased workload resulting from implementing CE, but it would allow for efficient alignment of resources in either situation or in response to other changes to reinvestigation policy and procedures.

Efficient robust results

As noted in the Secure Flight case study, reliability and efficiency refer to a model performing within a specified margin of error, minimizing false positives and false negatives. Throughout its evolution, ACES has been tested for performance against the traditional methods of investigation. Refinement of ACES business rules by adjudicators, security policy officials, and counter intelligence experts,[256] and the inclusion of additional datasets, has improved the efficiency of results.[257] The results of the studies performed by PERSEREC were so "promising"[258] that in 2001 the Office of the Secretary of Defense (OSD) encouraged continued development of ACES for implementation throughout the DOD. The actual business rules and performance statistics are not available in public documents, but the reliability of automated results from the ACES tool has been demonstrated and documented in multiple studies. As noted in PERSEREC documents, beta tests using ACES "found problems that investigators and

[255] Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf

[256] Eric L. Lang. *The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security*. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), September 2013).

[257] Ibid.

[258] Eric L. Lang. *The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security*. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), September 2013).

other sources had not previously identified."[259] Reliable results improve operational efficiency by enabling a more optimal allocation of resources. This benefits OPM and other investigative agencies by limiting the use of EFI or other resource intensive investigative procedures to only those cases where it is necessary.

b. Cost to Operations

The cost of research and development of ACES is difficult to compile. ACES has been in development for at least 10 years, and specific budget information for ACES versus other projects conducted by the Defense Personnel Security Research Center (PERSEREC) are not readily available in public documents.

It is reasonable to conclude that the ACES research and development represents a significant percentage of work conducted by PERSEREC. The Defense Human Resources Activity (DHRA) budget estimate for fiscal year 2014 lists the first two goals for PERSEREC as:

> Goal 1: Further develop a reliable and effective system for conducting automated data base checks to eliminate paper-based manual procedures and increase the availability of relevant personnel suitability and security information for the vetting and continuing evaluation of military and civilian personnel.
>
> Goal 2: Further develop automation and quality standards to improve the effectiveness of personnel suitability and security investigation processing and electronic adjudication of clean investigations.[260]

PERSEREC was established in 1986 to improve the "effectiveness, efficiency, and fairness"[261] of DOD personnel security systems. Department of Defense Directive 5210.79 (1992) reissued PERSEREC's mission to serve as the "DOD personnel security

---

[259] Ibid.

[260] U.S. Department of Defense, Defense Human Resources Activity. Fiscal Year 2014 Budget Estimates. (Washington, DC: Department of Defense, 2013). http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2014/budget_justification/pdf/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/DHRA_OP-5.pdf .

[261] Deputy Secretary of Defense, *Defense Personnel Security Research Center (PERSEREC)*, DOD Directive 5210.79.1. (Washington, DC: Deputy Secretary of Defense, 1992). http://fas.org/irp/doddir/dod/d5210_79.htm.

research center for the Department of Defense."[262] As noted in the DHRA Budget, PERSEREC's current work "supports the Performance Accountability Council" and reform of the personnel security clearance process.[263]

Documentation of costs to support PERSEREC is limited and difficult to compile. Budget estimates from DHRA cite annual budgets for PERSEREC as high as $6.5 million in fiscal year 2011,[264] falling to $1.2 million in fiscal year 2012, and averaging about $550,000 for fiscal years 2013 and 2014.[265] A Department of the Navy document cites PERSEREC's fiscal year 2008 budget as $9.1 million,[266] while DHRA documents state PERSEREC's budget for that same year was $1.1 million.[267] Older budgets have similar variability.[268]

The ACES system has been in development for at least 10 years. It has been designed by researchers from PERSEREC in Monterey, CA, and defense contractor Northrop Grumman.[269] An Associated Press report claims that ACES and "clearance-

---

[262] Ibid.

[263] U.S. Department of Defense, Defense Human Resources Activity. *Fiscal Year 2010 Budget Estimates*. (Washington, DC: Department of Defense, May 2009). http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2010/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PARTS/DHRA.pdf.

[264] U.S. Department of Defense, Defense Human Resources Activity. *Fiscal Year 2013 Budget Estimates*. (Washington, DC: Department of Defense, February 2012). http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2013/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PARTS/O_M_VOL_1_BASE_PARTS/DHRA_OP-5.pdf.

[265] U.S. Department of Defense, Defense Human Resources Activity. *Fiscal Year 2014 Budget Estimates*. (Washington, DC: Department of Defense, April 2013). http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2014/budget_justification/pdf/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/DHRA_OP-5.pdf.

[266] U.S Department of Defense, Department of the Navy. *Team Monterey Information & Statistics.* (Unknown: November 2009). http://www.public.navy.mil/fltfor/cnmoc/Documents/team_monterey_handouts.pdf .

[267] U.S. Department of Defense, Defense Human Resources Activity. *Fiscal Year 2010 Budget Estimates*. (Washington, DC: Department of Defense, May 2009). http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2010/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PARTS/DHRA.pdf.

[268] U.S. Department of Defense, Defense Human Resources Activity. *Fiscal Year (FY) 2004/FY 2005 Biennial Budget Estimates*. (Washington, DC: Department of Defense, February 2003). http://www.globalsecurity.org/military/library/budget/fy2004/dod/fy04pb_dhra.pdf.

[269] Stephen Braun. "U.S. intelligence officials to monitor federal employees with security clearances." *Associated Press.* March 10, 2014. http://www.pbs.org/newshour/rundown/us-intelligence-officials-monitor-federal-employees-security-clearances/.

related Defense Department research"[270] has cost more than $84 million[271] according to "documents"[272] that are not cited.

Direct contact with PERSEREC staff suggested that ACES development budgets were "contract sensitive" and not available in public documents. The online publication "ClearanceJobs.com" notes that there is "no clear explanation" for how ACES is or will be funded[273] and estimates the costs for the Department of Defense alone at approximately $53 million.[274]

The Security and Suitability Process Reform Strategic Framework, issued in February 2010, states that: "Resources from DOD and OPM are sufficient to enable implementation of the transformed process design for the mainstream elements of the process, as guided by the PAC."[275] This does not clarify the costs of implementing automated tools for clearance processing. However, it assigns the tasks of implementation of ARC, CE, and other technology modernizations to these agencies to accomplish within their respective budgets and notes that "funding has been identified by each of these entities to support planned reforms."[276]

Furthermore, the Office of Management and Budget (OMB) provided guidance for fiscal year 2015 that required the Departments of Justice, Treasury, and Homeland Security to "identify agency funding to prioritize automation requirements"[277] to enable CE capabilities. OMB has stated that it is developing a cost estimate for the expansion

---

[270] Stephen Braun. "U.S. intelligence officials to monitor federal employees with security clearances." *Associated Press.* March 10, 2014. http://www.pbs.org/newshour/rundown/us-intelligence-officials-monitor-federal-employees-security-clearances/.

[271] Ibid.

[272] Ibid.

[273] Lindy Kyzer. "OMB Releases Security Clearance Reform Report." ClearanceJobs.com. March 19, 2014. http://news.clearancejobs.com/2014/03/19/opm-releases-security-clearance-reform-report/.

[274] Ibid.

[275] U.S. Department of Homeland Security. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland (QHSR).* (Washington, DC: Department of Homeland Security, February. 2010). http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

[276] Ibid.

[277] Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

and implementation of CE beyond the DOD,[278] but values are not yet available. Finally, OMB also has required the DOD to "fund development of the CE capability leveraging the ACES platform."[279]

Costs are difficult to compile for ACES development and both past and future PERSEREC research. Given the nearly 18-year history of PERSEREC and at least 10-year history of ACES, annual budgets and other estimates would suggest that upwards of $100 million has been invested to date for research related to automated records checks for security clearance processing. Costs to expand pilot projects and fully develop and deploy CE capabilities could significantly add to what has already been invested.

However, the value of the existing research on ACES for the implementation of current programs is significant. Given the extensive history of research and testing already conducted on ACES, new projects need not take on full-scale testing. OPM and other agencies implementing ACES for ARC or CE programs will benefit from the investments made by DOD since PERSEREC began in 1986.

3. Effects of Automation on National Security

a. Benefits to National Security

Continuous Evaluation

Under the direction of the President, the Office of Management and Budget (OMB) conducted a review of the progress of clearance reform. OMB's review noted that:

> Current reinvestigation practices do not adequately reevaluate or appropriately mitigate risk within the security and suitability population. Lengthy periods between reinvestigations do not provide sufficient means to discover derogatory information that develops following the initial adjudication. Furthermore, resource constraints lead agencies to conduct fewer than the required number of reinvestigations.[280]

---

[278] Ibid.

[279] Ibid.

[280] Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

Continuous Evaluation (CE) remains a "vision" of the reformed security clearance process. It is not yet fully implemented. CE has been cited as a "critical element" for a robust security clearance process because of the long time intervals between periodic reinvestigations. As a result of these intervals, the government may be relatively uninformed as to behavior that poses a security or counterintelligence risk. Reducing this risk requires establishing an effective capability to assess an individual's continuing eligibility on a more frequent basis. *However, conducting this activity using manual checks or full field investigations would be* "inefficient and resource intensive,"[281] as noted by Brian A. Prioletti, an Assistant Director at ODNI, in an official statement to Congress. OPM Associate Director Dillaman believes that using ARC for CE is "a quick and cost effective method for assessing employees and supports a more robust continuous evaluation program."[282] Several CE pilots have been conducted or are underway as part of the JRE's continued efforts for clearance reform. These should be implemented with a full-range of ARC and supporting EFI or other procedures to ensure that national security information is safeguarded.

Prioletti and the JRE emphasize the importance of CE assessing an individual's eligibility to hold a security clearance or sensitive position on an ongoing basis. As a further sign of its importance, Executive Order 13467[283] and the revised Federal Investigative Standards authorized CE reviews of individuals in sensitive positions or with access to classified information "at any time" to ensure continued eligibility. CE initiatives could also deter "insider threats" by identifying unauthorized disclosures of classified information.

---

[281] Brian Prioletti. "Statement for the Record: Open Hearing on The Insider Threat to Homeland Security: Examining Our Nation's Security Clearance Processes." Counterterrorism and Intelligence Subcommittee of the Committee on Homeland Security. November 13, 2013. http://fas.org/irp/congress/2013_hr/111313prioletti.pdf. (Accessed July 20, 2014).

[282] Kathy L. Dillaman. Associate Director For Federal Investigative Services, Office of Personnel Management. *Personnel Security Clearance Reform.* Statement before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, United States House of Representatives. December 1, 2010. http://www.opm.gov/news/testimony/111th-congress/personnel-security-clearance-reform/.

[283] Executive Order no. 13467 of June 30, 2008, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information. *Code of Federal Regulations*, title 3, part 13467, (2008). http://www.ncix.gov/publications/policy/docs/EO_13467.pdf.

Given that ARC has been demonstrated to be effective in identifying issues at a low cost, implementing regular ARC as part of CE—such as ACES electronic database checks—between initial clearances and periodic reinvestigations may mitigate some risks to national security. ARC could identify factors like financial or criminal issues within the population of federal civilian and military employees before a 5-year or 10-year investigation.

Based on an ACES pilot of 3,370 Army uniformed, civilian, and contract employees that yielded precise and actionable results, the JRE plans to expand the use of ACES. The ODNI plans to develop capability to implement Continuous Evaluation (CE) for the most sensitive TS/SCI positions by the close of fiscal year 2014, with a full roll-out expected by 2016.[284] If completed, this expansion would likely reduce risks to national security.

Incorporating more data

ARC enables investigators to quickly review results from multiple data sources including government and commercial databases. Testing is underway to validate the use of additional information, such as screenings of social media. OPM states: "We are currently working with several new record repositories to establish agreements so that OPM can integrate these record checks into our investigations products."[285] Incorporating additional sources of information to include in automated checks could enhance the quality and content of the investigations by improving the robustness of results. As new data relevant to hiring and clearing decisions becomes available, automation enables this data to be incorporated into the records checks.[286] This has the

[284] Lindy Kyzer. "OMB Releases Security Clearance Reform Report." ClearanceJobs.com. March 19, 2014. http://news.clearancejobs.com/2014/03/19/opm-releases-security-clearance-reform-report/.

[285] Kathy L. Dillaman. Associate Director For Federal Investigative Services, Office of Personnel Management. *Personnel Security Clearance Reform.* Statement before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, United States House of Representatives. December 1, 2010. http://www.opm.gov/news/testimony/111th-congress/personnel-security-clearance-reform/.

[286] Joint Security and Suitability Reform Team. "Security and Suitability Process Reform." December 2008 http://www.whitehouse.gov/sites/default/files/omb/assets/omb/reports/joint_security_dec2008.pdf.

potential to improve the clearance process and enhance national security by identifying derogatory information from sources that were previously unavailable.

Prioletti addresses some of the challenges with incorporating certain types of additional data, such as activity on social media sites, in his statement to Congress. As Prioletti notes, pilot studies on the feasibility and utility of this data "identified actionable information," but "retrieving, analyzing, and processing"[287] it was resource intensive. Furthermore, there may be some privacy or civil liberties issues associated with incorporating this kind of information. Including additional information into ARC must be supported by policy, procedure, and the appropriate use of resources in order to maintain ARC as an efficient tool for supporting clearance processes.

Flexible, configurable systems

Observations from testing ACES note that it is "configurable" to different business rules, and that the system can be "calibrated" to check different sources or systems with different business rules depending on the nature of the investigation.[288] Similar comments have been made about Secure Flight as this is a feature common to DSS. Calibrating the ARC criteria or sensitivity thresholds may be done temporarily, in response to an elevated threat environment, or permanently, based on new policy, improved logic, or the availability of new information. When these characteristics are configured and applied universally, there are certainly operational efficiencies, such as the reduction of costs related to training and implementing new procedures. Further, universal application of new policies across an electronic system—rather than a human system—reduces the risk that new policies will be incorrectly communicated and followed. Flexibility and rapid responsiveness in systems configuration has a positive

[287] Brian Prioletti. "Statement for the Record: Open Hearing on The Insider Threat to Homeland Security: Examining Our Nation's Security Clearance Processes." Counterterrorism and Intelligence Subcommittee of the Committee on Homeland Security. November 13, 2013. http://fas.org/irp/congress/2013_hr/111313prioletti.pdf. (Accessed July 20, 2014).

[288] Eric L. Lang. *The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security*. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), September 2013).

effect on national security, and this is enabled by the use of ARC of electronic databases with an automated system such as ACES.[289]

b. Risks to National Security

Data Access Issues

The issue of access to data, such as the local police department records, is an important consideration when evaluating the benefits or risks to national security from utilizing ARC. Local records from the Seattle Police Department contained arrest information on Navy Yard Shooter Aaron Alexis. If investigators had access to this information during his initial or reinvestigations, this may have affected his clearance adjudication.[290]

Reliance on the results of ARC to enable EFI is only effective if investigators are confident that all relevant sources of information are included in the checks. That is, if a system of records cannot be included in ARC but the information contained in it would affect an adjudication, protocols must include checking this information in addition to the results of ARC. Efficiency is more optimal if the systems can be included, and OPM and other clearance investigators should pursue opportunities to include local law enforcement records or other relevant information in the ARC whenever possible. When it is not possible, thorough investigations to ensure national security should include protocols to manually check systems not included in ARC. Appropriate communication to field investigators that ARC is a tool that "supplements and does not replace"[291] investigations is important to maintain vigilance in the clearance process.

---

[289] Ibid.

[290] Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

[291] U.S. Department of Homeland Security, Office of Privacy. "Privacy Impact Assessment for the Automated Continuing Evaluation System (ACES) Pilot." (Washington, DC: Department of Homeland Security, April 9, 2007). http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_aces.pdf.

4. Findings

The fundamental factors for evaluating the policy decision to implement automation tools for immigration adjudication procedures as outlined in the methodology for this analysis are:

- expected benefits to stakeholders,
- potential improvements in operational efficiency, and;
- potential reduction of risks to national security.

The previous analysis shows that these factors are *substantially demonstrated* by the ACES system. This case study also supports the development and implementation of automation tools for immigration adjudications.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. AUTOMATION IN IMMIGRATION ADJUDICATIONS

A. ANALYSIS

In their 2012 analysis, "The Effects of USCIS Adjudication Procedures and Policies on Fraud Detection by Immigration Services Officers,"[292] the DHS OIG commented specifically on USCIS data systems. They noted that Immigration Services Officers (ISOs), in conducting background investigations on applicants for immigration benefits, must conduct "labor-intensive, system-by-system checks to verify or eliminate each possible match to terrorist watch lists and other derogatory information."[293] An earlier DHS OIG report in 2011 noted that this information on foreign nationals is fragmented among 17 data systems.[294]

In addition to national security systems or criminal records databases, ISOs may also need to query certain records systems[295] for verification of information provided in support of a benefit request. As noted in the Adjudicator's Field Manual (public redacted version) ISOs were responsible for querying applicant aliases one by one prior to a final decision: "Checks must be performed on additional names or alternate dates of birth that become known during the adjudicative process."[296] ISOs were required to review internal files and the results of records checks in order to analyze and determine whether an

---

[292] U.S. Department of Homeland Security, Office of Inspector General. *The Effects of USCIS Adjudication Procedures and Policies on Fraud Detection by Immigration Services Officers.* (OIG-12-24) (Washington, DC: Department of Homeland Security, January 2012). http://www.oig.dhs.gov/assets/Mgmt/OIG_12-24_Jan12.pdf.

[293] Ibid.

[294] U.S. Department of Homeland Security, Office of Inspector General. *Information Sharing on Foreign Nationals: Overseas Screening.* (OIG-11-68) (Washington, DC: Department of Homeland Security, April 2011). http://www.oig.dhs.gov/assets/Mgmt/OIGr_11-68_Apr11.pdf .

[295] U.S. Department of Homeland Security, United States Citizenship and Immigration Services. *Adjudicator's Field Manual—Redacted Public Version*. January 22, 2013. http://www.uscis.gov/iframe/ilink/docView/AFM/HTML/AFM/0-0-0-1.html.

[296] Ibid.

applicant had aliases or variations of his or her name and then initiate checks on all variations they discovered.[297]

As previously noted in this analysis, opportunities exist to improve the background investigations process through the use of automation and DSS.

B. COMPARISON TO CASE STUDIES

There are notable similarities between immigration adjudications processing and the two cases studied in this analysis. These are specified below to enable the extrapolation of expected benefits and costs of the proposal to implement automation and DSS in the immigration adjudications process.

Though there are differences depending on the type of immigration benefit being requested, processing generally follows these phases:

- *Application*. An individual submits an application for an immigration benefit. Depending on the type of benefit being requested, various supporting documentation or evidence is required. For certain requests, fingerprints or photos, called "biometrics," must be collected.

- *Investigation*. Using the information provided by the applicant in his or her clearance application materials, a background investigation of the applicant is conducted. Again, depending on the type of immigration benefit being requested, the depth of the investigation will vary. For many benefit types, the ISO will issue a "Request for Evidence" (RFE) to validate information provided by the applicant. Some benefit requests such as the form N-400 "Application for Naturalization" or form I-130, "Petition for Alien Relative," require interviews to inform the adjudication.

- *Adjudication*. After collecting all the necessary information, querying the appropriate systems, and potentially interviewing an applicant or petitioner, an ISO renders an adjudication on a request. The formal decision is written, and the decision notice is mailed and/or emailed to the applicant/petitioner. For some benefit types, adjudication may only involve a review of documentation for verification of eligibility.

[297] U.S. Department of Homeland Security, United States Citizenship and Immigration Services. *Adjudicator's Field Manual—Redacted Public Version*. January 22, 2013. http://www.uscis.gov/iframe/ilink/docView/AFM/HTML/AFM/0-0-0-1.html.

- *Post-Decision Activity*. After the denial of an immigration benefit request, many applicants have the opportunity to appeal. Not all denials are eligible for appeal, however. The appeals process is complex and may involve reinvestigation of an applicant. Other post-decision activities include document production (such as an I-551 "Legal Permanent Resident Card," or "Green Card") or an Oath Ceremony, as in the case of an approved naturalization decision.

The USCIS website, "My Case Status," is an interactive site for applicants or petitioners to get information related to their immigration benefit request. An immigration benefit request is often referred to by the Agency as a "case." The site describes several phases of processing, depicted in Figure 8.

Figure 8. USCIS "My Case Status" Processing Phases (from USCIS, 2014)[298]

The phase that the Agency calls "Initial Review" is the investigations phase of the overall process. The Agency describes this phase as follows:

> During this step, USCIS initiates the background checks of the applicant/ petitioner and identifies issues that may need to be addressed either during an interview or by asking the applicant/petitioner to submit additional information or documentation. USCIS reviews the applicant's/petitioner's criminal history, determines if there are national security concerns that need to be addressed, and reviews the application/petition for fraud indicators.[299]

[298] U.S. Department of Homeland Security, United States Citizenship and Immigration Services, "My Case Status." https://egov.uscis.gov/cris/Dashboard/CaseStatus.do.

[299] U.S. Department of Homeland Security, United States Citizenship and Immigration Services, "My Case Status Descriptions." https://egov.uscis.gov/cris/Dashboard/CaseStatus/BucketDescriptions.do#2.

This phase presents several elements to compare with the vetting of airline passengers against the terror watch lists and the processing of security clearances.

Multiple systems checks

As noted by the DHS OIG, an ISO might check up to 17 systems with multiple aliases or other derogatory information on an applicant for national security. In addition, the ISO might check several internal systems to verify data that is supplied by an applicant. This process is similar to the system checks conducted by Secure Flight and ACES in their automated processing. As previously noted, Secure Flight checks passenger names against the No Fly and Selectee lists. ACES was originally designed to check as many as 40 systems and can be calibrated to include or exclude systems depending on the type of investigation being conducted.

Aliases

As noted, the Adjudicator's Field Manual requires that an ISO check all discovered aliases in their investigation of an immigration benefit applicant. The use of aliases or spelling variations of an individual's name increases the workload required to complete the investigation. Although the exact rules-based queries for both Secure Flight and ACES are sensitive or classified and not available in public documents, both systems must process checks on the identities of individuals who may use different names or aliases. Secure Flight has initiated standard data formats to minimize false positives; ACES pilots have utilized commercial databases and credit reports to generate aliases and then used those additional names in records checks.[300] This element of background checking—the complication of queries based on name variations and aliases—is similar across all three processes.

Referrals

USCIS ISOs refer cases to Fraud Detection and National Security (FDNS) Immigration Officers (IOs) when their investigations reveal an articulable reason to

[300] U.S. Department of Homeland Security, Office of Privacy. "Privacy Impact Assessment for the Automated Continuing Evaluation System (ACES) Pilot." (Washington, DC: Department of Homeland Security, April 9, 2007). https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_aces.pdf .

suspect fraud or national security concerns.[301] FDNS IOs have access to additional national security commercial databases, and they may conduct other investigative activities to attempt to resolve a case.[302] This process is very similar to the referral processes in both watch list matching and security clearance processing. For passengers who match the No Fly or Selectee lists via the automated matching system used by Secure Flight, their information is referred to a Secure Flight Analyst to try to resolve the case or coordinate other investigative or law enforcement activities. Automated records checks conducted in a security clearance review may provide direction for an Expandable Focused Investigation (EFI).

A general model that can be derived from the two case studies can be represented by the flow chart in Figure 9.

[301] U.S. Department of Homeland Security, Office of Inspector General. *Review of the USCIS Benefit Fraud Referral Process (Redacted – Revised)*. (OIG-08-09) (Washington, DC: Department of Homeland Security, April 2008). http://www.oig.dhs.gov/assets/Mgmt/OIGr_08-09_Apr08.pdf.

[302] Ibid.

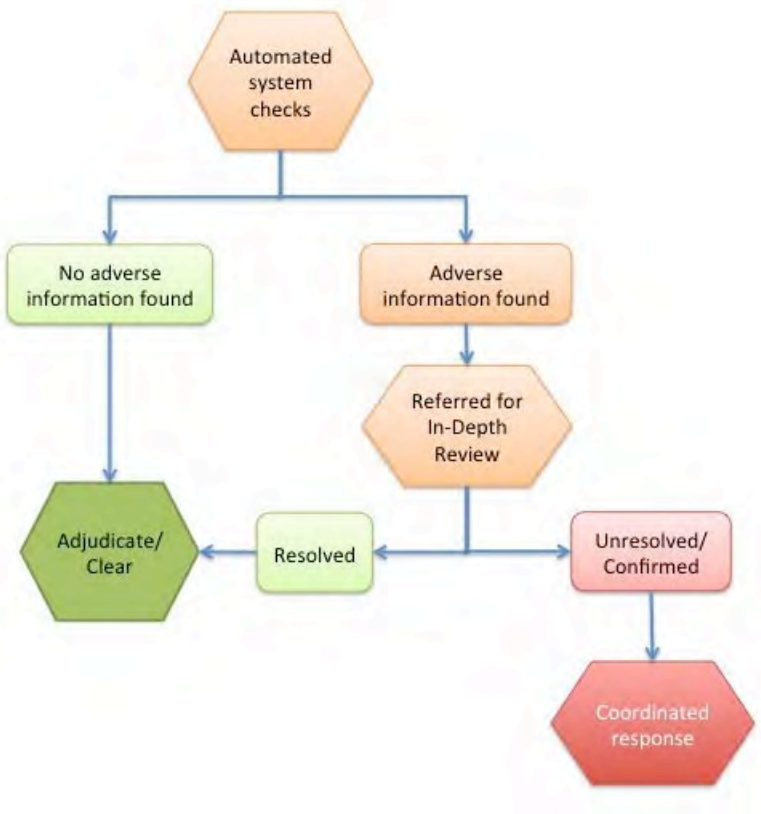

Figure 9. Use of Automation and Decision Support Tools in Investigative Procedures

This model can be directly translated to immigration adjudication procedures. Upon receipt of an immigration benefit request and beginning the "Initial Review" or investigative phase of the adjudications process, automated system checks could be used to sort cases with no adverse information to a queue for adjudications. Depending on the complexity of the review required for that request type, the potential exists for immediate or even fully automated adjudication. If adverse information is found, a case can be sorted for further review. If an ISO or IO was able to resolve the adverse information with more in-depth review, the case could then be adjudicated. If a resolution could not be made or if the concern was confirmed, USCIS could coordinate a response with the appropriate law enforcement or national security authorities to appropriately address the concern.

C. EXPECTED BENEFITS AND COSTS

As demonstrated, the model of automated system checks and referral procedures consequently applies to immigration benefit adjudications. The remaining questions, then, relate to the benefits and costs to stakeholders, the operational efficiencies, and the potential reduction of national security risks that could be realized if automation were implemented in immigration benefits adjudication.

As previously mentioned, these elements are fundamental factors in evaluating the policy decision to implement automation tools for immigration adjudication procedures. The examined cases demonstrate that significant resources are required to implement and support automation and decision support tools. Using the same framework through which benefits and costs of Secure Flight and ACES have been analyzed thus far, the following sections will analyze "expected" benefits and costs of implementing automation and decision support tools for immigration adjudications.

1. Benefits and Costs to Stakeholders

a. Benefits to Applicants/Petitioners

Faster and More Efficient Processing

As demonstrated in the cases, automation and DSS can reduce the overall amount of time required for investigatory procedures. Reducing the time between application and adjudication provides a customer service benefit to applicants. While the Agency currently processes applications according to a culture of customer service, reducing the wait time for all requests improves Agency's relationship with the immigrant community. For example, reuniting families faster or reducing the amount of time it takes to bring a petitioner's foreign spouse into the country benefits these applicants, though this is quite difficult to measure. The Agency also benefits from improved applicant and immigrant relations.

Further, if there were Agency policies and procedures that supported a "case flagging strategy" and that also supported expanded investigations only for applicants with derogatory information, an applicant might not be required to participate in an

investigatory interview. If an automated system were designed to minimize false positives, perhaps by incorporating more data elements like the Secure Flight system does, a DSS could produce more robust and reliable results. While this undoubtedly would benefit operations and national security, it would also benefit applicants who have names or aliases that are similar to those who are KST. It would appropriately identify them as having no derogatory information, and thus not subject them to expanded investigations.

Protecting Applicant Privacy

Requiring adjudicators to access as many as 17 national security systems and additional records systems indicates that the process incorporates risks to information security and individual privacy. Though ISOs are trained in privacy laws each year and required to sign "Rules of Behavior" documents that indicate the appropriate use of PII, risks of intentional or accidental privacy or security breaches increase with every additional system that is accessed. Keeping PII and national security information within a closed system with access controls enhances both security and privacy. Access controls on closed systems also provide mechanisms for deterring internal abuse, often referred to as "insider threats."[303]

b. Costs to Applicants/Petitioners

Compliance with data collection systems

The implementation of automated system checks could potentially involve the means for electronically collecting information from applicants. In this case, applicants and petitioners or their authorized representatives and attorneys would need to learn how to enter information into the system. The training time to learn the system and enter their information is a direct cost to this stakeholder group if it is more extensive than filing via current paper methods. Furthermore, any changes or updates to the system over time would require retraining.

[303] U.S. Office of the Director of National Intelligence, Office of the National Counterintelligence Executive. "Insider Threat." http://www.ncix.gov/issues/ithreat/. (Accessed August 4, 2014).

Processing Fees

If the Congress does not appropriate funds for the development of automation tools for immigration adjudications, the Agency might need to raise funds for its development. USCIS might raise fees to maintain Agency operations, transferring some of the cost to applicants. It is difficult to estimate these potential costs. Indeed the possibility exists that the implementation of automation will have such a positive impact on Agency operations that fee increases will be unnecessary.

Personal Privacy Concessions

Implementing an automated decision support tool for checking national security databases in support of current policies and procedures would have a neutral effect on privacy relative to the amount of information that adjudicators access on any individual. However, if additional information were incorporated into automated records checks—due to the ease of calibration or availability of additional data sources—privacy regulations or documents may need to be updated.

Applicants for immigration benefits acknowledge that their personal information may be accessed and reviewed when they sign and submit a request form. That being said, it is likely that privacy advocacy groups would have negative commentary on the incorporation of additional data into the adjudications process as a violation of privacy rights.

2. Costs and Benefits to USCIS Operations from Automation in Immigration Adjudications

a. Benefits to Operations

Productivity Improvements

Simply relieving officers of the need to check multiple systems will have a positive impact on their productivity by reducing the amount of time it takes to conduct an adjudication. There are additional benefits of utilizing an automated, centralized system for records checks related to training and access to systems.

Though there may be an initial training investment when an automated system is first deployed, minimizing the number of systems that adjudicators are required to access will reduce systems-related training hours in the long run. This applies to onboarding training as well as training due to system updates or periodic training as required by the Agency for access to sensitive systems. Furthermore, policy changes can impact training requirements. To the extent that policies can be translated into business rules that are programmed into an automated system, training to ensure compliance might also be reduced.

Furthermore, time spent managing access to systems, such as recalling usernames or updating passwords, is minimized when automation centralizes system checks. As noted by the DHS OIG, access issues like lockouts, automatic logoffs, and varying password cycles makes managing access to multiple systems a time-consuming challenge.[304]

DHS OIG noted that there is some potential for risk to information security and privacy when "officers whose passwords have lapsed ask their DHS colleagues to conduct searches for them."[305] A serious potential outcome is that an officer might forego certain system checks due to the difficulty in the process and thus not fully consider all available information in a case. This analysis will address consistency in checking all systems as well as calibrating a system to universally incorporate policy changes as benefits to national security in later sections.

Resource alignment

As previously analyzed with respect to Secure Flight and ACES, the use of a "case flagging strategy" may offer improvements to Agency operations due to the efficient alignment of resources that this strategy enables. The process outlined in Figure 9 demonstrates how this strategy is relevant for immigration adjudications. Previous

[304] U.S. Department of Homeland Security, Office of Inspector General. *The Effects of USCIS Adjudication Procedures and Policies on Fraud Detection by Immigration Services Officers.* (OIG-12-24) (Washington, DC: Department of Homeland Security, January 2012). http://www.oig.dhs.gov/assets/Mgmt/OIG_12-24_Jan12.pdf.

[305] Ibid.

analysis on this strategy for adjudications procedures for aviation security and clearance processing is applicable to immigration adjudications. The robustness of results further enhances the efficiency of resource alignment, and the Agency would do well to sufficiently test and refine the criteria and business rules that are incorporated into automated queries.

Expansion of Agency Processing Capacity

As noted, USCIS experienced a change in procedures in 2003 and an increase in receipts in advance of the changes to the N-400. The Agency will continually be subject to external factors impacting workload and procedures, not the least of which is the possibility of CIR. Both the Secure Flight and ACES cases demonstrate that DSS and automation enable and support high-capacity processing. The Secure Flight system vets as many as 14 million passengers each week.[306] The ACES system was originally tested with small samples of data in pilot projects, but was "greatly expanded"[307] in scope when the JRE prioritized automation. The volume of checks processed by ACES technology increased significantly.

This thesis does not evaluate the capacity of the technological systems used for automation in the cases. However, the number and quality of system interfaces, the bandwidth of networks, and the processing capacity of information technology systems would all impact the speed at which automated checks could be performed. Systems analysts could determine the optimal capacity of these items to enable fast processing of background check information in immigration adjudications.

b. Costs to Operations

Investment of Resources

As with Secure Flight and ACES, the development and implementation of an automation tool for system and records checks for immigration adjudications will have

[306] U.S. Department of Homeland Security, "Preventing Terrorism and Enhancing Security." July 8, 2013. http://www.dhs.gov/preventing-terrorism-and-enhancing-security. (Accessed May 26, 2014).

[307] Eric L. Lang. *The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security*. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), September 2013).

real costs in dollars and other resources. As noted by DHS OIG in a 2014 report on information technology (IT) management, USCIS's IT spending in fiscal year 2012 totaled approximately $379 million.[308] While this value covers all IT spending throughout the Agency, including operations and maintenance costs on existing systems as well as hardware maintenance and replacement costs, this is not an insignificant budget.

USCIS is currently undertaking a large-scale IT development and implementation program called "Transformation" that is intended to "modernize USCIS by transitioning the Agency from a fragmented, paper-based environment to a centralized, paperless environment using electronic adjudication."[309] The system that is being developed, called "USCIS ELIS," is a candidate platform in which to incorporate automated system and records checks. In fact, in USCIS ELIS was originally envisioned to include this functionality. As noted by DHS OIG in a progress review of the program in 2012, USCIS ELIS was originally planned to "fully automate the entire benefits process, such as automatically assigning work to USCIS employees and automatically checking for potential criminal and fraudulent activity."[310] "Automated fraud detection"[311] through a "risk analyzer"[312] was intended to address issues related to the use of different names and aliases by individuals attempting to circumvent fraud and national security system checks."[313] DHS OIG noted:

---

[308] U.S. Department of Homeland Security, Office of Inspector General. *U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges*. (OIG-14-112) (Washington, DC: Department of Homeland Security, July 2014). http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-112_Jul14.pdf.

[309] Ibid.

[310] U.S. Department of Homeland Security, Office of Inspector General. *U.S. Citizenship and Immigration Services' Progress in Transformation*. (OIG-12-12) (Washington, DC: Department of Homeland Security, November 2011). http://www.oig.dhs.gov/assets/Mgmt/OIG_12-12_Nov11.pdf.

[311] U.S. Department of Homeland Security, Office of Inspector General. *The Effects of USCIS Adjudication Procedures and Policies on Fraud Detection by Immigration Services Officers.* (OIG-12-24) (Washington, DC: Department of Homeland Security, January 2012). http://www.oig.dhs.gov/assets/Mgmt/OIG_12-24_Jan12.pdf.

[312] Ibid.

[313] Ibid.

> We were informed that the risk analyzer will identify all aliases, which will provide greater protection for the immigration system. Transformation will provide access to data from the applicant, USCIS data systems, and any aliases discovered from other immigration and law enforcement data systems. The system will identify aliases much more efficiently than ISO review of paper files, according to a Transformation official.[314]

As of July 2014, the "risk analyzer" has not been deployed. USCIS has "extended the timeline for its initial deployment of electronic capabilities"[315] and "reduced the scope of the deployment."[316] Even in the absence of deploying an automated "risk analyzer," USCIS has invested significant resources into USCIS ELIS.

A reliable aggregate value of spending on USCIS ELIS is difficult to come by. DHS OIG reported obligations of more than $500 million between fiscal years 2008 and 2011.[317] Its review in 2014 noted costs of over $1.7 billion for a 6-year period.[318] The White House IT Dashboard notes that the Agency spent $176.4 million for fiscal year 2014 alone.[319] USCIS furnished values for a required report known as the "Exhibit 300" with a "Total Cost" including government employee salaries of $569.5 million.[320]

---

[314] U.S. Department of Homeland Security, Office of Inspector General. *The Effects of USCIS Adjudication Procedures and Policies on Fraud Detection by Immigration Services Officers.* (OIG-12-24) (Washington, DC: Department of Homeland Security, January 2012). http://www.oig.dhs.gov/assets/Mgmt/OIG_12-24_Jan12.pdf.

[315] U.S. Department of Homeland Security, Office of Inspector General. *U.S. Citizenship and Immigration Services' Progress in Transformation.* (OIG-12-12) (Washington, DC: Department of Homeland Security, November 2011). http://www.oig.dhs.gov/assets/Mgmt/OIG_12-12_Nov11.pdf.

[316] Ibid.

[317] Ibid.

[318] Judicial Watch Blog Corruption Chronicles. "6 Years, $1.7 Bil Later DHS Visa System Deemed Failure." *Judicial Watch.* August 11, 2014. http://www.judicialwatch.org/blog/2014/08/6-years-1-7-bil-later-dhs-visa-system-deemed-failure/. (Accessed August 12, 2014).

[319] White House, Federal IT Dashboard. "USCIS - Transformation." https://www.itdashboard.gov/investment?buscid=319. (Accessed August 2, 2014).

[320] U.S. Department of Homeland Security, United States Citizenship and Immigration Services. *Exhibit 300: Capital Asset Summary, USCIS – Transformation.* (Washington, DC: Department of Homeland Security, July 2014). https://it-2014.itdashboard.gov//investment/exhibit300/pdf/024-000003015.

Whatever the exact cost of the development and implementation of the USCIS ELIS system, the work of developing, testing, and deploying the originally intended "risk analyzer" tool or some similar automated tool will add to this investment.

Opportunity cost

The basic definition of "opportunity cost" is the "value of the next-highest-valued alternative"[321] or the value of what a resource could be used for instead of its current use. The obligation of a significant amount of resources and funding towards the development of an automated tool for system and records check would preclude the use of those resources and funds for other reasons. The latest USCIS Fiscal Year Accomplishments Brochure (2012) notes a wide range of initiatives from developing and implementing procedures for the administrative relief program "Deferred Action for Childhood Arrivals" (DACA), to launching the first phase of USCIS ELIS, as well as several humanitarian programs.[322] The availability of resources for these and other initiatives at the Agency would be limited by their obligation towards the development of automation tools.

3. Effects of Automation in Immigration Adjudications on National Security

a. Benefits to National Security

Recency and frequency of records checks

Automation would offer a significant improvement in the recency and frequency of the records checks that are considered during an immigration adjudication. This would reduce risks of fraud or threats to public safety and national security. The public redacted version of the USCIS Adjudicator's Field Manual indicates that system checks must be conducted within 90 days of a decision on an application. If an adjudicator runs the

---

[321] David R. Henderson, "Opportunity Cost." *The Concise Encyclopedia of Economics*. (Online: Library of Economics and Liberty, 2008). http://www.econlib.org/library/Enc/OpportunityCost.html

[322] U.S. Department of Homeland Security, United States Citizenship and Immigration Services. *USCIS Accomplishments Fiscal year 2012*. (Washington, DC: Department of Homeland Security, 2013). http://www.uscis.gov/sites/default/files/USCIS/About%20Us/Budget%2C%20Planning%20and%20Performance/USCIS%20FY2012%20Accomplishments%20Brochure.pdf.

manual checks, then issues a Request for Evidence (RFE), places the case in a pending status, and then revisits that case 88 days later, the results of the system checks would be valid to process the decision. Given the constant workload on USCIS adjudicators and the fact that rechecks are not required within 90 days, it is unlikely that the checks would be regularly reprocessed. This recency gap in information poses a significant risk to public safety and national security. If records checks were automated and results were returned quickly, rechecks could be conducted immediately before an adjudicator renders a decision. As an example, immediately before taking the oath of naturalization, candidates for citizenship must attest that since their last interview, they have not committed crimes or been arrested, per the Form N-445 "Notice of Naturalization Oath Ceremony."[323] This mini-interview is conducted on the site of a naturalization ceremony where adjudicators generally have no access to verify the information being attested. If automated records checks were available, the entire group of applicants could be rechecked immediately prior to naturalization, which could identify risks to public safety or national security. This benefit to national security is similar to the benefit provided by continuous evaluation (CE) in security clearances.

Consistently checking all systems with programmable variations in aliases

In a 2012 review of USCIS adjudications procedures, the DHS OIG noted significant challenges that adjudicators faced with manual system checks. DHS OIG noted that:

> Challenges in alias identification are compounded because USCIS uses cumbersome and outdated immigration data systems. Both USCIS employees and some law enforcement agency users express frustration with USCIS systems. Our recent report on overseas screening noted that information on foreign nationals is fragmented among 17 data systems. Officers must conduct labor-intensive, system-by-system checks to verify

[323] See U.S. Department of Homeland Security, United States Citizenship and Immigration Services, Form N-445 "Notice of Naturalization Oath Ceremony." http://www.ilw.com/forms/N445.pdf.

> or eliminate each possible match to terrorist watch lists and other derogatory information.[324]

Further, in a 2014 review of USCIS information technology investments, the DHS OIG noted that:

> USCIS staff members are not always sure of which systems to use or which systems are available to them to complete business processes. For example, staff members in some locations were not aware that they should be using the Arrival and Departure Information System (ADIS) during the adjudication process. ADIS is a DHS Office of Biometric Identity Management system used to collect and maintain the arrival and departure information of non-U.S. citizens traveling to the U.S. A high level official in the field learned about the value of the system when a Fraud Detection and National Security supervisor brought it to the official's attention.[325]

Non-standard system use is a risk to national security. USCIS Officials interviewed by DHS OIG expressed concerned that "if every site is not using the same systems, applicants could travel to different field offices to receive different results."[326]

As demonstrated with the Secure Flight and ACES systems and discussed previously, automation offers improvements to consistency over manual system-by-system checks on multiple aliases. Automation would reduce variability in procedures related to checking aliases. Further, automation would ensure that all systems are checked for every applicant, as a system can be designed to incorporate all relevant systems containing information on foreign nationals and internal records systems. These characteristics of automated systems offer improvements to national security related to consistency.

---

[324] U.S. Department of Homeland Security, Office of Inspector General. *The Effects of USCIS Adjudication Procedures and Policies on Fraud Detection by Immigration Services Officers.* (OIG-12-24) (Washington, DC: Department of Homeland Security, January 2012). http://www.oig.dhs.gov/assets/Mgmt/OIG_12-24_Jan12.pdf.

[325] U.S. Department of Homeland Security, Office of Inspector General. *U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges*. (OIG-14-112) (Washington, DC: Department of Homeland Security, July 2014). http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-112_Jul14.pdf.

[326] U.S. Department of Homeland Security, Office of Inspector General. U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges. (OIG-14-112) (Washington, DC: Department of Homeland Security, July 2014). http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-112_Jul14.pdf.

Referring fraud and national security issues

In a review conducted in 2008, DHS OIG noted that USCIS policies and procedures contained disincentives for ISOs to identify and refer fraud cases.[327] The current referral process is labor-intensive. Given that certain Agency performance metrics rate ISOs on their productivity based on numerical formulas for expected case completions, ISOs might not be referring all suspected cases of fraud.[328] Automation could ensure that any evidence of fraud or national security risks found in system checks were flagged and referred to an FDNS IO. There are certainly bases for fraud referrals not found in systems checks that ISOs may uncover during interview procedures, and automation would not necessarily affect these referrals. However, an automated system for system check referrals might also include tools to simplify other referral procedures. In either scenario, automation offers an improvement over current procedures.

USCIS already has referral procedures for situations when serious threats to public safety or national security are identified in their investigations processes. Automation may offer the capacity to improve coordination with enforcement agencies or local law enforcement, as it has with Secure Flight.

Incorporating more data

ACES has been tested with the inclusion of as many as 40 systems, and it can be calibrated to include or exclude systems based on business rules determined by process experts. As previously noted, automation in immigration adjudications could enable consistent inclusion of all currently available systems. This alone offers improvements to inconsistent system checks. As demonstrated through ACES testing, when new data relevant to immigration adjudications becomes available, automation enables this data to be incorporated into the records checks.[329] The inclusion of additional sources of

---

[327] U.S. Department of Homeland Security, Office of Inspector General. *Review of the USCIS Benefit Fraud Referral Process (Redacted – Revised).* (OIG-08-09) (Washington, DC: Department of Homeland Security, April 2008). http://www.oig.dhs.gov/assets/Mgmt/OIGr_08-09_Apr08.pdf.

[328] U.S. Department of Homeland Security, Office of Inspector General. *Review of the USCIS Benefit Fraud Referral Process (Redacted – Revised).* (OIG-08-09) (Washington, DC: Department of Homeland Security, April 2008). http://www.oig.dhs.gov/assets/Mgmt/OIGr_08-09_Apr08.pdf.

[329] Joint Security and Suitability Reform Team. "Security and Suitability Process Reform." December 2008. http://www.whitehouse.gov/sites/default/files/omb/assets/omb/reports/joint_security_dec2008.pdf .

information could mean the corroboration of derogatory information and improve the quality of decisions. However, the inclusion of additional information into immigration adjudications would likely involve a change in policy and procedure and updates to privacy regulations and documents.

Flexibility and uniformity

As noted for both Secure Flight and ACES, automation offers flexibility in system calibration. This applies to its potential use in immigration adjudications, as well. An automated system supporting immigration adjudications could be quickly calibrated in response to an elevated threat environment based on policy or procedures changes. The new rules would be applied universally across all applicants as soon as the system was reprogrammed. While responses to threats or policies can be implemented in its absence, automation offers rapid response and uniform application, thus improving national security.

Privacy and Information Security Controls

Previously noted as a benefit to applicants, improvements to information security and privacy controls also benefit national security. Requiring adjudicators or IOs to access as many as 17 national security systems and additional records systems incorporates risks to information security and individual privacy. Utilizing an automated system that conducts queries without manual review by adjudicators reduces the risk of data exposure and deters internal abuse.

Risk-Based Models

As early as 2002, Lee S. Strickland and Jennifer Willard suggested the use of data mining and risk analyses to completely reengineer the immigration adjudications process.[330] Rather than develop decision support tools to streamline current immigration adjudication procedures, they suggested a more radical approach to investigating applicants. They proposed using powerful data mining tools to develop risk profiles

[330] Lee S. Strickland and Jennifer Willard. "Reengineering the Immigration System: A Case for Data Mining and information Assurance to Enhance Homeland Security." Bulletin of the American Society for Information Science and Technology 29, no.1 (2002): 16–21.

based on applicant characteristics. This proposal to reengineer the immigration system is more drastic than simply automating existing procedures. However, they argued that rules-based procedures are inadequate for protecting national security from potential terrorists.[331] These procedures for adjudication would utilize risk assessments now being used by Secure Flight to support expedited or enhanced pre-screening procedures.

The use of advanced analytics and data mining tools to collect "positive" information on applicants, rather than simply running checks for "negative" information, is not possible without the use of automation and decision support tools. Employing this type of risk-based adjudications throughout USCIS would require significant policy analysis and regulation to implement. It might require an act of Congress. Full analysis of privacy and security issues would also be necessary.

Risk-based investigations might offer the Agency additional operational efficiencies, as it has for TSA. These efficiencies and potential improvements to national security are only feasible with an automated system in place.

b. Risks to National Security

False documents and false identities

As previously noted, issues with false identities and false documents pose a risk for aviation security, and automation does not improve it. There is a similar risk of the use of false documents in immigration applications, which also relies on the accuracy of the information that applicants submit. Many immigration applications require significant evidentiary support, and each piece of required evidence is an opportunity for an applicant to submit something fraudulent. Adjudicators are trained to look for signs of document fraud, but sophistication in falsifying documents can make them hard to detect for even experienced adjudicators.

[331] Lee S. Strickland and Jennifer Willard. "Reengineering the Immigration System: A Case for Data Mining and information Assurance to Enhance Homeland Security." Bulletin of the American Society for Information Science and Technology 29, no.1 (2002): 16–21.

Many immigration applications require the collection of biometrics such as photographs and fingerprints.[332] Once these are collected, an applicant's identity is at least consistent throughout the rest of the process. Certain immigration benefits require an interview, thus offering another opportunity for identify verification. USCIS recently implemented a verification tool called "Customer Identity Verification"[333] which it uses whenever an applicant appears in person. Automated records checks in support of current immigration adjudication procedures would neither improve nor worsen the risk of document or identity fraud.

However, automated records checks offer an opportunity to decrease the risk of document fraud with certain changes to the process. For documents or data that are produced or stored by the other agencies of the United States federal government, such as arrival or departure records from CBP, USCIS could circumvent document fraud opportunities by requesting direct access to the databases. Rather than requiring adjudicators to review possibly fraudulent documents submitted by applicants, an automated system could query the authoritative sources directly. This type of inter-agency information sharing may be necessary to ensure national security and deter fraud and arguably falls under investigations exemptions to the Privacy Act. However, updates to privacy regulations might be required to support automated records checks or advanced analytics of applicant data.

4. Findings

The fundamental factors for evaluating the policy decision to implement automation tools for immigration adjudication procedures as outlined in the methodology for this analysis are:

- expected benefits to stakeholders,

[332] U.S. Department of Homeland Security, United States Citizenship and Immigration Services. "Photographs and Fingerprints." May 3, 2010. http://www.uscis.gov/forms/file-my-application-online-e-filing/photographs-and-fingerprints. (Accessed August 4, 2014).

[333] U.S. Department of Homeland Security, United States Citizenship and Immigration Services. "USCIS Implements Customer Identity Verification at Field Offices." September 19, 2013. http://www.uscis.gov/uscis-tags/unassigned/uscis-implements-customer-identity-verification-field-offices. (Accessed August 4, 2014).

- potential improvements in operational efficiency, and
- potential reduction of risks to national security.

The previous analysis shows that these factors could be *substantially achieved* by the development and implementation of automation tools for immigration adjudications.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

A. COMPREHENSIVE IMMIGRATION REFORM CONTEXT

As with most new government activities that result from new laws or policies, the development, implementation, and operation of decision support tools for immigration adjudications will involve monetary and opportunity costs. Expenditures to support the automation of adjudications will require the endorsement, buy-in, participation, and cooperation of several essential stakeholders.

This thesis demonstrates that the Agency could realize benefits for operational efficiency and national security by implementing automation, and these benefits remain valid even in the absence of immigration reform. It is important to consider the current context for immigration adjudications: at this time, Comprehensive Immigration Reform (CIR) is a significant factor in resource planning for the next several years for USCIS. Considering the implementation of automation is relevant in this context.

As of this publication, an immigration reform bill has not been passed by Congress. An available benchmark for considering the impact of immigration reform can be found in the "Border Security, Economic Opportunity, and Immigration Modernization Act," also known as S. 744,[334] passed by the United States Senate in July 2013. Many issues related to immigration reform are still up for debate, and until the United States House of Representatives or full Congress proposes another option, S. 744 is the only available tool for analysis at this time.

With a few exceptions, immigration benefit requests require applicants or petitioners to pay fees to process their applications. While a small number of USCIS directorates operate on budgets that are appropriated by Congress, revenues generated from application fees fund the majority of USCIS's operations. In bill S. 744, $750,000,000[335] is allocated to expand the employment verification system, "eVerify,"

[334] Border Security, Economic Opportunity, and Immigration Modernization Act, S.744, 113th Cong., 1st sess. (2013). http://www.gpo.gov/fdsys/pkg/BILLS-113s744es/pdf/BILLS-113s744es.pdf.

[335] Ibid.

which is operated by one of the appropriated directorates of USCIS.[336] The bill also provides that a new benefit category be created and fees be collected with associated applications. USCIS could expect to recoup certain operational costs from the fees collected with these applications. However, S. 744 does not provide any up front funding for USCIS to expand its adjudication operations in advance of its implementation. Based on current estimates of the undocumented immigrant population in the United States, USCIS predicts an influx of applications that would triple the agency's current workload when immigration reform passes. USCIS is aware of this oversight of advance operational funding. However, despite the projected increase in workload, the Agency may have limited incentive to implement significant operational changes now because it could leverage operational deficiencies for necessary funding. Compounding this is the fact that the political environment surrounding immigration reform remains uncertain.

There are a few possible outcomes for the future of immigration adjudications. In one scenario, immigration reform or some presidential action will affect immigration policy, and USCIS will use existing manual processes for system and records checks. Workloads will increase for all officers, operational efficiency will decrease, and there will be significant impacts to customer service and national security. In another scenario, USCIS or the Congress will have the foresight to fund and implement automation as a decision support tool for the Agency to prepare for the additional workload. This thesis argues that automation as a decision support tool can improve national security even in the absence of future immigration reform legislation. However, given the cost and challenge of developing an automation tool, immigration legislation could certainly draw sufficient attention to motivate its implementation.

B. STAKEHOLDERS IN THE IMPLEMENTATION OF AUTOMATION

1. Americans and Immigration Applicants

The political environment of immigration adjudications involves a wide range of players. These include the American citizenry and millions of "future voters," several

[336] U.S. Department of Homeland Security, United States Citizenship and Immigration Services. "E-Verify." http://www.uscis.gov/e-verify. (Accessed July 23, 2014).

federal agencies and their leadership including USCIS, the union of employees at USCIS, and the Congress. In this space, those essential to championing the changes required to develop, implement, and use automation as a decision-support tool for immigration adjudications include USCIS Agency leadership, the Congress, and the union of USCIS employees. Those influential to implementing such a program include other federal agency partners. Those who are nominal or interchangeable in the process are the American citizenry, present and future.

The American public is a direct beneficiary of any effort to improve the quality of immigration adjudications through operational efficiencies and the use of risk-based analytics. If immigration reform is considered a given, which it is not, the applicants for a new status created by CIR would also be direct beneficiaries of efficient procedures since they would not be able to exercise the benefits granted to them (lawful status and work permits) until their applications were processed. Those supporting the immigrant community, such as the large body of lawfully present Mexicans and Latin Americans, as well as voting citizens formerly from parts of the world largely represented in the undocumented population, are also nominal beneficiaries of operational efficiencies at USCIS.

Processing times—how long it takes to process a particular benefit request—and production rates—how many decisions an office produces—are public indicators of Agency operational efficiency. When processing times become excessive, the results are public dissatisfaction and risks to national security in the form of insufficient investigations on applicants for the sake of speed. USCIS regularly publishes information related to processing times in order to address concerns from the public and especially from those that represent them. The American Immigration Lawyers Association (AILA) has been tracking processing time reports from USCIS on its website since 1996.[337] While USCIS indicates that customer service is central to its mission, fast processing times are not a true goal. These processing issues could be used to leverage money from Congress, particularly if the Agency is expected to respond to new immigration

[337] American Immigration Lawyers Association, AILA InfoNet. "CSC Processing Time Reports." http://www.aila.org/content/default.aspx?bc=6740. (Accessed July 2, 2014).

legislation without advance or additional funding. Indeed, this is precisely the case with the version of the immigration reform bill, S.744, which passed the United States Senate.

That being said, the present and future citizenry have little influence over the Agency's decision to use or not to use automation as a decision-support tool. If processing times became excessive or if there were a significant national security event as a direct result of an incorrect adjudication due to insufficient investigations, the American public might voice concerns to representatives in Congress. As will be discussed later, Congress is an essential partner in implementing automation as a decision support tool.

2. Other Federal Agencies

Other federal agencies are influential to the decision to implement automation tools at USCIS. Some of the systems that immigration adjudicators must query to process a benefit request are "owned" by other agencies, such as the National Crime Information Center (NCIC) system, which is maintained by the Federal Bureau of Investigations, a part of the Department of Justice; or the Student & Exchange Visitor Information System (SEVIS), which is maintained by Immigration and Customs Enforcement (ICE). In order to fully automate background check queries for immigration adjudications, cooperation and technology investment will be required of these agencies. If the Congress requires the development and use of automation tools for immigration adjudications, building the technological interfaces will require these agencies to work together. In this scenario, successful relationships among these organizations will warrant prioritization.

3. USCIS Leadership

In order to support and fund the development of an automated system for adjudications, Agency leaders will need to understand the national security risks of current operations and the potential paralyzing impact of slow processing times that will result from a significantly increased workload at USCIS. As with the two cases analyzed in this thesis, both Secure Flight and ACES became prioritized only after major security issues resulted from poor operations. The Intelligence Reform and Terrorism Prevention Act (IRPTA) of 2004 was passed by Congress in part to enact several recommendations

of the 9/11 Commission Report. Though the population that will be eligible for benefits created by immigration reform may pose less risk to national security than others, it is important to realize that the increased adjudications workload will have an impact on all agency operations and all benefit request types. Investigations not conducted in a thorough or timely fashion may permit those who seek to harm us easier entry into our country. This will impact our national security.

Backlogged cases are a customer service issue, as previously discussed. Indeed, a large Agency effort in 2006 known as the "Backlog Elimination Plan" specifically focused on reducing cases that were pending adjudication. In 2003, changes in adjudications procedures mandated additional background checks and expanded the range of applicants that were required to submit fingerprints and other biometrics in support of their applications.[338] These operational changes resulted in a peak backlog of 3.85 million cases in January 2004.[339] Former Agency Director Dr. Emilio T. Gonzalez made regular presentations concerning efforts to reduce the backlog to several Congressional committees. His last presentation on the subject included acknowledgement of "the thousands of USCIS employees who came in early, stayed late and worked weekends" to meet agency production goals without compromising "quality or integrity."[340] Agency employees working overtime completed all of this work manually. A backlog of 3.85 million cases represents a little more than half of the agency's current workload of 6 to 7 million cases per year.

An approximation of the workload impact of S.744 must take into consideration the compound nature of the process that would be created to support Lawful Prospective Immigrant (LPI) status, involving initial applications for status and work authorization, as well as status reapplications and citizenship applications as outlined in the Bill. The

[338] U.S. Department of Homeland Security, United States Citizenship and Immigration Services. *Backlog Elimination Plan: Fiscal Year 2006, 3rd Quarter Update*. (Washington, DC: Department of Homeland Security, December 11, 2006). http://www.uscis.gov/sites/default/files/USCIS/Resources/Reports%20and%20Studies/backlog_FY06Q3.pdf.

[339] Ibid.

[340] Ibid.

initial influx of applications could be 11–12 million;[341] however, the evidentiary requirements of LPI status and the supplementary application for employment authorization compound the issue of simply tripling receipts of applications. Furthermore, the Bill requires reapplication after 6 years, thus increasing the workload baseline. Per S.744, LPI become eligible to apply for citizenship after 10 years, and naturalized U.S. Citizens are then eligible to petition for family members to immigrate to the U.S. or adjust status to lawful permanent residents (LPR). Each of these procedures requires USCIS adjudication resources, thus supporting the prediction of a permanent increase in the Agency's workload.

Though using overtime resources was successful in 2004 for eliminating a backlog of an additional 50% of typical workload, it would have little effect on a growing backlog of this magnitude. Options for the Agency might include permanently increasing staffing levels or implementing process changes such as automation decision support tools. Both would involve significant approval procedures at the level of the Congress or White House.

As discussed earlier, different immigration benefit types pose varying levels of adjudicative and processing burdens on the Agency. Depending on the complexity of the application, the evidentiary requirements, and other characteristics of any new status created by CIR, the workload impact will vary. Based on an evaluation of the requirements outlined in S.744, the LPI status would rate among the more complex "adjustment of status" applications as defined in section 245 of the Immigration and Nationality Act, 8 U.S.C. 1255.[342]

4. The Congress

Politics surrounding immigration reform are contentious. As a result, members of Congress and political organizations could impact the implementation of automation

[341] Jeffrey S. Passel, D'Vera Cohn, and Ana Gonzalez-Barrera. "Population Decline of Unauthorized Immigrants Stalls, May Have Reversed." *Pew Research Hispanic Trends Report*. September 23, 2013. http://www.pewhispanic.org/2013/09/23/population-decline-of-unauthorized-immigrants-stalls-may-have-reversed/.

[342] *Immigration and Nationality Act, U.S. Code 8* (1952), § 1255. http://www.gpo.gov/fdsys/pkg/USCODE-2011-title8/pdf/USCODE-2011-title8-chap12-subchapII-partV-sec1255.pdf .

tools at USCIS. Those who support immigration reform in general might support appropriations for operational improvements at USCIS to process the influx of applications. Those who oppose immigration reform might object to appropriations for operational improvements at USCIS in an effort to undermine the overall implementation of CIR. While it is feasible that USCIS could assume the responsibility for the development and deployment of automation tools to support immigration adjudications without an act of Congress, direct inclusion of USCIS operational changes in immigration reform legislation might ensure its success.

5. Union of USCIS Employees

The Union of USCIS employees is a significant stakeholder in the implementation of automation tools. Funding, development, and implementation of automation decision support tools are wasted if the tool is not utilized. At USCIS, some past attempts to implement large-scale technologies to improve agency operations have faced opposition from the employee union.

Any changes to job duties for immigration officers—those who review and adjudicate immigration benefit requests—must be negotiated or bargained. Agency culture related to job performance metrics, job requirements and reviews, and adjudicator caseload is regularly a topic of union discussions. The Union successfully prevented the implementation of certain elements of the Enterprise Performance Analysis System (ePas) in 2011 and again in 2012.[343] Current Agency efforts to develop and deploy an electronic case management system and adjudications platform called "USCIS ELIS" (Electronic Immigration System)[344] face regular renegotiations on bargaining agreements.[345]

---

[343] U.S. Department of Homeland Security, United States Citizenship and Immigration Services, Office of Performance and Quality. "OPQ News." April 4, 2013. http://connect.uscis.dhs.gov/news/Documents/uscis_today_OPQNews.htm.

[344] U.S. Department of Homeland Security, United States Citizenship and Immigration Services. "USCIS ELIS." April 16, 2014. http://www.uscis.gov/uscis-elis.

[345] U.S. Department of Homeland Security, Office of Inspector General. *U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges.* (OIG-14-112) (Washington, DC: Department of Homeland Security, July 2014). http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-112_Jul14.pdf.

However, immigration reform might provide an opportunity for the Agency to leverage burdensome workloads to implement decision support tools. Mr. Kenneth Palinkas, the president of the American Federation of Government Employees Council 119, which represents officers and staff at USCIS, criticized S. 744 stating that it "will damage public safety and national security" because it was unlikely that immigration officers would be afforded the appropriate time for "diligent case review" and "proper investigation into red flags."[346] Labor unions are motivated by job security and pay security. Given the expected increase in workload with CIR, job security becomes moot, and the Agency's task of negotiating the implementation of decision support tools becomes easier.

Though this thesis demonstrates that the implementation of a decision support tool in the absence of CIR would help improve immigration officers' capacity to conduct "diligent case reviews" and "proper investigations," it is likely that the union would view such a tool as a threat to officer job security.

C. RECOMMENDATIONS

The fundamental factors for evaluating the policy decision to implement automation tools for immigration adjudication procedures—expected benefits to stakeholders, improvements to operational efficiency, and the reduction of risks to national security—have been demonstrated in the preceding analysis. Therefore, this thesis recommends their development.

1) USCIS should develop automation tools for immigration adjudications regardless of the status of immigration reform or other immigration policy changes.

As discussed, there are a few possible outcomes for the future of immigration adjudications. Generally speaking, there are two variables to consider when evaluating the need for automation tools for immigration: changes in policy or procedure and changes in workload. Policy and procedure can be affected on a large scale by external

[346] American Federation of Government Employees Council 119. "USCIS Union President: Lawmakers Should Oppose Senate Immigration Bill, Support Immigration Service Officers." May 20, 2013. http://graphics8.nytimes.com/packages/pdf/Reform0520USCISCouncilLet.pdf.

factors like acts of Congress or the President, or on a smaller scale by internal factors like Agency leadership decisions. Changes in workload can be affected by many external factors, including the availability of new benefit types per new law or executive order; international crises (war, political unrest, natural disasters, or other) that affect immigration patterns; seasonal or cyclical increases in application receipts; and many others. Each of these factors carries an inherent probability or likelihood which itself may change over time due to external factors. Over the course of existence of USCIS since 2003, each of these external or internal factors has come to pass in one way or another. Each instance has had an operational impact on the Agency and an effect on national security.

Consequently, it is reasonable to assume that, even in the absence of specific probability rates for each possible factor, something external will affect operations at USCIS. This thesis has shown that automated tools to support adjudication and investigative procedures can improve operational responsiveness to such factors. For USCIS, operational efficiency and responsiveness support meeting its goals, as outlined in Mission 3 of the QHSR: to effectively and efficiently administer immigration laws; provide prompt and accurate adjudications; prevent fraud, abuse, and exploitation; eliminate systemic vulnerabilities; and prevent the entry of criminals or dangerous foreign nationals.[347]

2) If the Congress or the President makes changes to immigration policy, funding specifically to support the development of automation tools at USCIS should be allocated.

Given the cost and the challenge of developing an automation tool, resource constraints at USCIS will limit progress towards its implementation. Current efforts to develop an electronic application, a case management system, and the adjudications platform called "USCIS ELIS" under the Transformation Program are already

[347] U.S. Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland (QHSR)*. (Washington, DC: Department of Homeland Security, February. 2010). http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

significantly behind original plans, both in schedule and budget.[348] While automated records checks could reasonably fit into the development of USCIS ELIS, the funding and resources to build it properly would need to be evaluated for priority among all other Agency information technology efforts.

As previously noted, operational inefficiencies or customer service problems that are likely to arise due to the expected workload impact of CIR provide the Agency with leverage for additional funding. However, an operational efficiency gap of this magnitude would pose a significant national security risk. Therefore, Congress or the White House should fund the development of an automation tool for immigration adjudications in conjunction with significant changes to immigration policy or procedure.

[348] White House, Federal IT Dashboard. "USCIS ELIS." https://www.itdashboard.gov/investment?buscid=319. (Accessed August 8, 2014).

LIST OF REFERENCES

American Airlines. "TSA Secure Flight Information Is Required To Travel." n.d. http://www.aa.com/i18n/utility/secureFlight.jsp?anchorLocation=DirectURL&title=secureflight. (Accessed May 25, 2014).

American Civil Liberties Union (ACLU). "The Four Biggest Problems With the 'Secure Flight' Airline Security Program." March 4, 2005. https://www.aclu.org/technology-and-liberty/four-biggest-problems-secure-flight-airline-security-program. (Accessed May 25, 2014).

American Federation of Government Employees Council 119. "USCIS Union President: Lawmakers Should Oppose Senate Immigration Bill, Support Immigration Service Officers." May 20, 2013. http://graphics8.nytimes.com/packages/pdf/Reform0520USCISCouncilLet.pdf.

American Immigration Lawyers Association. "CSC Processing Time Reports." *AILA InfoNet*. http://www.aila.org/content/default.aspx?bc=6740. (Accessed July 2, 2014).

Anthony, R. (1965). *Planning and Control Systems: A Framework for Analysis*. (Cambridge, MA: Harvard University Graduate School of Business Administration, 1965).

Border Security, Economic Opportunity, and Immigration Modernization Act, S.744, 113th Cong., 1st sess. (2013). http://www.gpo.gov/fdsys/pkg/BILLS-113s744es/pdf/BILLS-113s744es.pdf.

Braun, S. (2014)."U.S. intelligence officials to monitor federal employees with security clearances." *Associated Press*. March 10, 2014. http://www.pbs.org/newshour/rundown/us-intelligence-officials-monitor-federal-employees-security-clearances/.

Ceruti, M., Wilcox, D. & Powers, B. (2004). Space and Naval Warfare Systems Center, San Diego, CA. "Knowledge Management for Command and Control." *Paper for the 2004 Command and Control Research and Technology Symposium*, June 15–17, 2004.

Christensen, M. & Kaiser, F. (2013). *Security Clearance Process: Answers to Frequently Asked Questions*. (CRS Report RL R43216) (Washington, DC: Office of Congressional Research Service, September 9, 2013). http://fas.org/sgp/crs/secrecy/R43216.pdf.

Code of Federal Regulations, *Privacy Act of 1974: Implementation of Exemptions; Secure Flight Records*, title 49, sec. 1507. http://www.dhs.gov/xlibrary/assets/privacy/privacy_nprm_tsa_secureflight.pdf.

Code of Federal Regulations, *Secure Flight Program; Final Rule*, title 49, sec. 154. October 28, 2008. http://www.gpo.gov/fdsys/pkg/FR-2008-10-28/html/E8-25432.htm.

Defense Personnel and Security Research Center (PERSEREC). "Past Achievements." http://www.dhra.mil/perserec/pastachievements.html#ACES_2014. (Accessed July 5, 2014).

———. "Current Initiatives." http://www.dhra.mil/perserec/currentinitiatives.html. (Accessed June 24, 2014).

Delta Airlines. "Secure Flight Passenger Data (SFPD) FAQs." October 8, 2010. http://www.delta.com/content/www/en_US/agency/useful-resources/secure-flight-passenger-data-faqs.html. (Accessed May 22, 2014).

Deputy Secretary of Defense, Defense Personnel Security Research Center (PERSEREC), DOD Directive 5210.79.1. (Washington, DC: Deputy Secretary of Defense, 1992). http://fas.org/irp/doddir/dod/d5210_79.htm.

Dillaman, K. (2010). Associate Director For Federal Investigative Services, Office of Personnel Management. *Personnel Security Clearance Reform*. Statement before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, United States House of Representatives. December 1, 2010. http://www.opm.gov/news/testimony/111th-congress/personnel-security-clearance-reform/.

Eisler, P. & Vanden Brook, T. (2013). "Security clearances: Holes in the system?" *USA Today*. September 30, 2013. http://www.usatoday.com/story/news/nation/2013/09/30/problems-with-security-clearances/2897303/. (Accessed July 5, 2014).

Electronic Frontier Foundation. "Comments of the Electronic Frontier Foundation." September 24, 2007. https://www.eff.org/files/filenode/travelscreening/092407_secure_flight_comments.pdf. (Accessed July 25, 2014).

EPIC – Electronic Privacy Information Center. "Secure Flight." EPIC. http://www.epic.org/privacy/airtravel/secureflight.html. (Accessed July 19, 2014).

Executive Order no. 12968 of August 4, 1995, Access to Classified Information. *Code of Federal Regulations*, title 3, part 12968, (1995). http://www.ncix.gov/publications/policy/docs/EO_12968.pdf.

Executive Order no. 13467 of June 30, 2008. "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information." *Code of Federal Regulations*, title 3, part 13467, (2008). http://www.ncix.gov/publications/policy/docs/EO_13467.pdf.

Gorry, G. & Morton, M. (1971). "A Framework for Management Information Systems." *Sloan Management Review* 13, no. 1 (1971): 50–70.

Hasbrouck, E. (2004). "Why CAPPS-II would cost a billion dollars." *The Practical Nomad*, February 13, 2004. http://hasbrouck.org/blog/archives/000149.html.

Henderson, D. (2008). "Opportunity Cost." *The Concise Encyclopedia of Economics*. (Online: Library of Economics and Liberty, 2008). http://www.econlib.org/library/Enc/OpportunityCost.html.

Immigration and Nationality Act, U.S. Code 8 (1952), § 1255. http://www.gpo.gov/fdsys/pkg/USCODE-2011-title8/pdf/USCODE-2011-title8-chap12-subchapII-partV-sec1255.pdf.

Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA), Pub. L. No. 108–458, 118 Stat. 3638 (Dec. 17, 2004), codified at 42 U.S.C. §2000ee, 50 U.S.C. §403-1 et seq., §403-3 et seq., §404o et. seq.

Jackson, B., Chan, E. & LaTourrette, T. (2011). "Assessing the Security Benefits of a Trusted Traveler Program in the Presence of Attempted Attacker Exploitation and Compromise." (Santa Monica, CA: Rand Corp., May 2011). http://www.rand.org/content/dam/rand/pubs/working_papers/2011/RAND_WR855.pdf. (Accessed July 11, 2014).

Jelassi, M., Jarke, M. & Stohr, E. (1985). "Designing a Generalized Multiple-Criteria Decision Support System." *Journal of Management Information Systems* 1 (Spring 1985):4.

Joint Security and Suitability Reform Team. "Security and Suitability Process Reform." December 2008. http://www.whitehouse.gov/sites/default/files/omb/assets/omb/reports/joint_security_dec2008.pdf.

Joint Security and Suitability Reform Team. *Security and Suitability Process Reform Initial Report.* April 30, 2008. http://www.whitehouse.gov/sites/default/files/omb/reports/reform_plan_report_2008.pdf.

Judicial Watch Blog Corruption Chronicles. "6 Years, $1.7 Bil Later DHS Visa System Deemed Failure." *Judicial Watch*. August 11, 2014. http://www.judicialwatch.org/blog/2014/08/6-years-1-7-bil-later-dhs-visa-system-deemed-failure/. (Accessed August 12, 2014).

Kyzer, L. (2014). “OMB Releases Security Clearance Reform Report.” ClearanceJobs.com. March 19, 2014. http://news.clearancejobs.com/2014/03/19/opm-releases-security-clearance-reform-report/.

Lang, E. (2007). *Adjudication Decision Support (ADS) System Automated Approval Estimates for NACLC Investigations, Technical Report 07–04.* (Monterey, CA: Defense Personnel Security Research Center (PERSEREC), May 2007). http://www.dhra.mil/perserec/reports/tr07-04.pdf.

———. (2013).*The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security*. (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC), September 2013). http://www.dhra.mil/perserec/reports/TR%2013-06%20ACES%20Evolution.pdf.

London, R. (2014). “Secure Flight Will Not Use Commercial Databases.*” Privacy Security Law Blog*. http://www.privsecblog.com/2005/09/articles/policy-regulatory-positioning/secure-flight-will-not-use-commercial-databases/. (Accessed July 19, 2014).

Marshall, P. (2014). “Secure Flight’s off-the-shelf recipe.” *GCN*. http://gcn.com/articles/2011/10/17/tsa-secure-flight-tech-sidebar.aspx. (Accessed May 11, 2014).

McAfee, A. & Brynjolfsson, E. “Big Data: The Management Revolution.” *Harvard Business Review*, 90, no. 10 (October 2012): 60–68.

Moore, J. (2014). Federal News Radio Online. “White House backs 13 recommendations to improve security clearance process.” March 19, 2014. http://www.federalnewsradio.com/520/3585372/White-House-backs-13-recommendations-to-improve-security-clearance-process. (Accessed July 11, 2014).

National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report.* (New York: W.W. Norton & Co., 2004).

NBC News.com, “How Secure Flight Works.” http://www.nbcnews.com/id/39892975/ns/travel-travel_tips/t/how-secure-flight-works/. (Accessed June 1, 2014).

Nelson, L. & Smith-Pritchard, S. (2013). *Baseline Suitability Analysis. Technical Report 13–05.* (Monterey, CA: Defense Personnel and Security Research Center (PERSEREC). July 2013). https://www.hsdl.org/?view&did=751526.

Passel, J., Cohn, D. & Gonzalez-Barrera, A. (2013). “Population Decline of Unauthorized Immigrants Stalls, May Have Reversed.” *Pew Research Hispanic Trends Report*. September 23, 2013. http://www.pewhispanic.org/2013/09/23/population-decline-of-unauthorized-immigrants-stalls-may-have-reversed/.

Prioletti, B. “Statement for the Record: Open Hearing on The Insider Threat to Homeland Security: Examining Our Nation’s Security Clearance Processes.” Counterterrorism and Intelligence Subcommittee of the Committee on Homeland Security. November 13, 2013. http://fas.org/irp/congress/2013_hr/111313prioletti.pdf. (Accessed July 20, 2014).

Privacy Act, U.S. Code 5 (1974), § 522a. http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf.

“Privacy Act of 1974: Implementation of Exemptions and System of Records; Secure Flight Records; Final Rule and Notice,” *Federal Register* 7, no. 217 (November 9, 2007), 63706. http://www.gpo.gov/fdsys/pkg/FR-2007-11-09/pdf/E7-21907.pdf.

Security and Suitability Performance Accountability Council (PAC). *Security and Suitability Process Reform Strategic Framework.* (Washington, DC: Security and Sustainability Performance Accountability Council, February 2010). http://www.nationalsecuritylaw.org/files/received/OMB/Security_and_Suitability_Process_Reform-Strategic_Framework.pdf.

Shim, J., Warkentin , M., Courtney, J., Power, D., Sharda, R. & Carlsson, C. (2002). “Past, present, and future of decision support technology.” *Decision Support Systems* 33, no. 2 (2002): 111–126.

Simon, H. (1960). “The New Science of Management Decision,” in *The Ford Distinguished Lectures,* Volume 3. (New York, NY: Harper & Brothers, 1960).

Strickland, L. & Willard, J. (2002). “Reengineering the Immigration System: A Case for Data Mining and Information Assurance to Enhance Homeland Security.” *Bulletin of the American Society for Information Science and Technology* 29, no.1 (2002): 16–21.

Suitability and Security Process Review Report to the President. February 2014. http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

Toor, Amar. (2014). “PreCheck unchecked: why the TSA is putting more people in the fast lane.” *The Verge*. January 14, 2014. http://www.theverge.com/2014/1/14/5307000/why-is-the-tsa-pushing-everyone-through-precheck-security-screening. (Accessed July 11, 2014).

U.S Department of Defense, Department of the Navy. *Team Monterey Information & Statistics*. (Unknown: November 2009). http://www.public.navy.mil/fltfor/cnmoc/Documents/team_monterey_handouts.pdf.

U.S. Department of Defense, Defense Human Resources Activity. *Fiscal Year (FY) 2004/ FY 2005 Biennial Budget Estimates.* (Washington, DC: Department of Defense, February 2003). http://www.globalsecurity.org/military/library/budget/fy2004/dod/fy04pb_dhra.pdf.

———. *Fiscal Year 2010 Budget Estimates.* (Washington, DC: Department of Defense, May 2009). http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2010/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PARTS/DHRA.pdf.

———. *Fiscal Year 2013 Budget Estimates*. (Washington, DC: Department of Defense, February 2012). http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2013/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PARTS/O_M_VOL_1_BASE_PARTS/DHRA_OP-5.pdf.

———. *Fiscal Year 2014 Budget Estimates.* (Washington, DC: Department of Defense, May 2013). http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2014/budget_justification/pdf/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/DHRA_OP-5.pdf.

U.S. Department of Homeland Security, "Preventing Terrorism and Enhancing Security." July 8, 2013. http://www.dhs.gov/preventing-terrorism-and-enhancing-security. (Accessed May 26, 2014).

U.S. Department of Homeland Security, Office of Inspector General. *Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program (redacted version).* (OIG-09-103) (Washington, DC: Department of Homeland Security, September 2009). http://www.oig.dhs.gov/assets/Mgmt/OIG-09-103r_Sep09.pdf.

———. *Implementation and Coordination of TSA's Secure Flight Program (redacted version).* (OIG-12-94) (Washington, DC: Department of Homeland Security, July 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf.

———. *Information Sharing on Foreign Nationals: Overseas Screening.* (OIG-11-68) (Washington, DC: Department of Homeland Security, April 2011). http://www.oig.dhs.gov/assets/Mgmt/OIGr_11-68_Apr11.pdf.

———. *Review of the USCIS Benefit Fraud Referral Process (Redacted – Revised).* (OIG-08-09) (Washington, DC: Department of Homeland Security, April 2008). http://www.oig.dhs.gov/assets/Mgmt/OIGr_08-09_Apr08.pdf.

———. *Role of the No Fly and Selectee Lists in Securing Commercial Aviation (redacted version).* (OIG-09-64) (Washington, DC: Department of Homeland Security, July 2009). http://www.oig.dhs.gov/assets/Mgmt/OIGr_09-64_Jul09.pdf.

———. *The Effects of USCIS Adjudication Procedures and Policies on Fraud Detection by Immigration Services Officers.* (OIG-12-24) (Washington, DC: Department of Homeland Security, January 2012). http://www.oig.dhs.gov/assets/Mgmt/OIG_12-24_Jan12.pdf.

———. *U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges*. (OIG-14-112) (Washington, DC: Department of Homeland Security, July 2014). http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-112_Jul14.pdf.

———. *U.S. Citizenship and Immigration Services' Progress in Transformation.* (OIG-12-12) (Washington, DC: Department of Homeland Security, November 2011). http://www.oig.dhs.gov/assets/Mgmt/OIG_12-12_Nov11.pdf.

U.S. Department of Homeland Security, Office of Privacy. "Privacy Impact Assessment." (Washington, DC: Department of Homeland Security, April 9, 2007). http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight.pdf.

———. "Privacy Impact Assessment for the Automated Continuing Evaluation System (ACES) Pilot." (Washington, DC: Department of Homeland Security, April 9, 2007). https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_aces.pdf.

———. "Privacy Impact Assessment Update for Credential Authentication Technology/ Boarding Pass Scanning System. DHS/TSA/PIA-024(b)." (Washington, DC: Department of Homeland Security, January 18, 2013). http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia%20update_tsa_cat%20bpss_20130118.pdf.

———. "Privacy Impact Assessment Update for Secure Flight DHS/TSA/PIA - 018(e)." (Washington, DC: Department of Homeland Security, April 13, 2012). http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight_update018%28e%29.pdf.

———. "Report to the Public on the Transportation Security Administration's Secure Flight Program and Privacy Recommendations." (Washington, DC: Department of Homeland Security, December 2006). http://www.dhs.gov/xlibrary/assets/privacy/privacy-secure-flight-122006.pdf.

U.S. Department of Homeland Security, Transportation Security Administration, Office of Acquisition. "Official Solicitation for the TSA Secure Flight Resolution Center, call center support." Solicitation No. HSTS02-08-R-TTC159. July 3, 2008. https://www.fbo.gov/index?tab=documents&tabmode=form&subtab=core&tabid=ed9d723a863da7938300737ab3358e07.

U.S. Department of Homeland Security, Transportation Security Administration, Transportation Sector Network Management. "Regulatory and Economic Analysis. Regulatory Evaluation: Secure Flight Final Rule (49 CFR 1560)." October 17, 2008. http://www.papersplease.org/_dl/sf/Secure_Flight_regulatory_assessment.pdf.

U.S. Department of Homeland Security, Transportation Security Administration. "Mission, Vision, and Core Values." January, 2014. http://www.tsa.gov/about-tsa/mission-vision-and-core-values. (Accessed May 26, 2014).

———. "Privacy Act of 1974: Implementation of Exemptions; Secure Flight Records." *Federal Register 72*, no. 163 (August 23, 2007): 48357, August 23, 2007. http://www.gpo.gov/fdsys/pkg/FR-2007-08-23/pdf/E7-15963.pdf.

———. "Risk-Based Security Initiatives." February 10, 2014, http://www.tsa.gov/traveler-information/tsa-risk-assessments. (Accessed May 26, 2014).

———. "Secure Flight Communications Toolkit: Talking Points for Editorial from TSA." July 20, 2010, Version 3.0. http://www.tsa.gov/content/communications-toolkit. (Accessed June 1, 2014).

———. "Secure Flight Overview." March 19, 2014, http://www.tsa.gov/stakeholders/secure-flight-program. (Accessed May 26, 2014).

———. "Secure Flight Program." http://www.tsa.gov/stakeholders/secureflight-program. (Accessed January 21, 2014).

———. "Secure Flight: Frequently Asked Questions." March 19, 2014. http://www.tsa.gov/content/frequently-asked-questions-secure-flight. (Accessed May 26, 2014).

———. "Secure Flight: Your Safety is our Priority." Presentation to Global Business Travel Association (GBTA) Conference. April 22, 2009. http://www.gbta.org/Lists/Resource%20Library/NBTAWebinar_SecureFlight.pdf

U.S. Department of Homeland Security, United States Citizenship and Immigration Services. Form N-445, "Notice of Naturalization Oath Ceremony." http://www.ilw.com/forms/N445.pdf.

———. "Adjudicator's Field Manual—Redacted Public Version." January 22, 2013. http://www.uscis.gov/iframe/ilink/docView/AFM/HTML/AFM/0-0-0-1.html.

———. "E-Verify." http://www.uscis.gov/e-verify. (Accessed July 23, 2014).

———. "Photographs and Fingerprints." May 3, 2010. http://www.uscis.gov/forms/file-my-application-online-e-filing/photographs-and-fingerprints. (Accessed August 4, 2014).

———. "USCIS Implements Customer Identity Verification at Field Offices." September 19, 2013. http://www.uscis.gov/uscis-tags/unassigned/uscis-implements-customer-identity-verification-field-offices. (Accessed August 4, 2014).

———. *Backlog Elimination Plan: Fiscal Year 2006, 3rd Quarter Update.* (Washington, DC: Department of Homeland Security, December 11, 2006). http://www.uscis.gov/sites/default/files/USCIS/Resources/Reports%20and%20Studies/backlog_FY06Q3.pdf.

———. *Exhibit 300: Capital Asset Summary, USCIS – Transformation.* (Washington, DC: Department of Homeland Security, July 2014). https://it-2014.itdashboard.gov//investment/exhibit300/pdf/024-000003015.

———. *USCIS Accomplishments Fiscal Year 2012.* (Washington, DC: Department of Homeland Security, 2013). http://www.uscis.gov/sites/default/files/USCIS/About%20Us/Budget%2C%20Planning%20and%20Performance/USCIS%20FY2012%20Accomplishments%20Brochure.pdf.

U.S. Department of Homeland Security. *Advance Passenger Information System Pre-Departure Final Rule & Secure Flight Notice of Rule Making.* (Washington, DC: Department of Homeland Security, n.d.). http://www.hlswatch.com/sitedocs/apis-secure-flight-joint-faqs.pdf.

———. *Annual Performance Report, Fiscal Years 2012 – 2014.* (Washington, DC: Department of Homeland Security, April 2013). http://www.dhs.gov/sites/default/files/publications/MGMT/DHS-%20Annual%20Performance%20Report%20and%20Congressional-Budget-Justification-FY2014.pdf.

———. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland (QHSR).* (Washington, DC: Department of Homeland Security, February 2010). http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

U.S. Government Accountability Office. *Assessments of Selected Complex Acquisitions.* (GAO-10-588SP) (Washington, DC: GPO, 2010). http://www.gao.gov/assets/210/204132.pdf.

———. *Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program.* (GAO-06-864T) (Washington, DC: GPO, 2006). http://www.gao.gov/products/GAO-06-864T.

———. *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks.* (GAO-09-292) (Washington, DC: GPO, 2009). http://www.gao.gov/products/GAO-09-292.

———. *High-Risk Series: An Update.* (GAO-05-207) (Washington, DC: GPO, 2005). http://www.gao.gov/products/GAO-05-207.

———. *Homeland Security Acquisitions: DHS Could Better Manage Its Portfolio to Address Funding Gaps and Improve Communications with Congress*. (GAO-14-332) (Washington, DC: GPO, 2014). http://www.gao.gov/products/GAO-14-332.

———. *More Accurate Estimate of Overdue Security Clearance Reinvestigations is Needed*. (GAO/T-NSIAD-00-246) (Washington, DC: GPO, 2000). http://gao.gov/assets/110/108657.pdf.

———. *Personnel Security Clearances: An Outcome-Focused Strategy Is Needed to Guide Implementation of the Reformed Clearance Process*. (GAO-09-488) (Washington, DC: GPO, 2009). http://www.gao.gov/products/GAO-09-488.

———. *Personnel Security Clearances: Continuing Leadership and Attention Can Enhance Momentum Gained from Reform Effort.* (GAO-12-815T) (Washington, DC: GPO, 2012). http://gao.gov/assets/600/591784.pdf.

———. *Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum*. (GAO-11-65) (Washington, DC: GPO, 2011). http://www.gao.gov/products/GAO-11-65.

———. *Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed*. (GAO-05-256) (Washington, DC: GPO, 2005). http://www.gao.gov/products/GAO-05-256.

———. *Terrorist Watchlist: Routinely Assessing Impacts of Agency Actions since the December 25, 2009, Attempted Attack Could Help Inform Future Efforts.* (GAO-12-476) (Washington, DC: GPO, 2012). http://www.gao.gov/assets/600/591312.pdf.

Welsh, T. (2005). "The Security Risks of Modern Distributed Systems." CSO Online. November 9, 2005. http://www.csoonline.com/article/2119090/data-protection/the-security-risks-of-modern-distributed-systems.html. (Accessed July 11, 2014).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California