NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEPARTMENT OF HOMELAND SECURITY AND USCG FINANCIAL MANAGEMENT SYSTEM MODERNIZATION, CHALLENGES AND OPPORTUNITIES

by

Nguyentrinh E. Hoang

September 2021

Thesis Advisor: Cristiana Matei
Second Reader: Jon Watson,
U.S. Coast Guard

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
DEPARTMENT OF HOMELAND SECURITY AND USCG FINANCIAL MANAGEMENT SYSTEM MODERNIZATION, CHALLENGES AND OPPORTUNITIES

5. FUNDING NUMBERS

6. AUTHOR(S) Nguyentrinh E. Hoang

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

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

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

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

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

In 2017, after three years of investment, the Department of Homeland Security (DHS) restarted an IT acquisition project focused on the U.S. Coast Guard's (USCG) and Transportation Security Administration's financial system. Such projects bear inherent risks in terms of their size and interoperability and affect a wide range of agencies' operational missions. This thesis conducts a comparative analysis of the DHS's financial system failure and examines whether this project failure shares characteristics and challenges with other large government IT projects. It analyzes the causes, risks, and ways to mitigate IT failures through four case studies of large government IT projects that failed: DHS's financial system, the USCG electronic health care system, the HealthCare.gov website, and the FBI virtual case file program. It finds that these IT projects share common challenges, including significant schedule delays and cost increases, which inevitably led them to fail. The four case studies reveal a few important elements that contribute to successful government IT projects: defining the project outcomes at the beginning, having the right expertise, leading the organization through business process change, and fostering internal control procedures. These findings are representative of a small sample size , only cover recent IT projects in the United States. Future research can focus on the lessons learned from the failures to benefit both public and private IT development projects.

14. SUBJECT TERMS financial management system, acquisition, business process and project management	**15. NUMBER OF PAGES** 115
	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.

DEPARTMENT OF HOMELAND SECURITY AND USCG FINANCIAL MANAGEMENT SYSTEM MODERNIZATION, CHALLENGES AND OPPORTUNITIES

Nguyentrinh E. Hoang
Senior Budget Analyst, USCG, Department of Homeland Security
BA, University of California - Santa Cruz, 2002
MBA, Defense Systems Analysis, Naval Postgraduate School, 2005

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

NAVAL POSTGRADUATE SCHOOL
September 2021

Approved by: Cristiana Matei
Advisor

Jon Watson
Second Reader

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

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In 2017, after three years of investment, the Department of Homeland Security (DHS) restarted an IT acquisition project focused on the U.S. Coast Guard's (USCG) and Transportation Security Administration's financial system. Such projects bear inherent risks in terms of their size and interoperability and affect a wide range of agencies' operational missions. This thesis conducts a comparative analysis of the DHS's financial system failure and examines whether this project failure shares characteristics and challenges with other large government IT projects. It analyzes the causes, risks, and ways to mitigate IT failures through four case studies of large government IT projects that failed: DHS's financial system, the USCG electronic health care system, the HealthCare.gov website, and the FBI virtual case file program. It finds that these IT projects share common challenges, including significant schedule delays and cost increases, which inevitably led them to fail. The four case studies reveal a few important elements that contribute to successful government IT projects: defining the project outcomes at the beginning, having the right expertise, leading the organization through business process change, and fostering internal control procedures. These findings are representative of a small sample size; they only cover recent IT projects in the U.S. Future research can focus on the lessons learned from the failures to benefit both public and private IT development projects.

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

ACA	Affordable Care Act
ACS	Automated case support system
ADA	Anti-Deficiency Act
ADE	Acquisition Decision Event
AHLTA	Armed Forces Health Longitudinal Technology Application
AoA	Analysis of Alternatives
CAS	Core Accounting System
CHCS	Composite Health Care System
CHIP	Children's Health Insurance Program
CIO	Chief Information Officer
CMS	Centers for Medicare & Medicaid Services
CONOPS	Concepts of Operations
COT	Commercial-off-the-shelf
CWMD	Countering Weapons of Mass Destruction Office
DHS	Department of Homeland Security
DSH	Federal Data Service Hub
DOD	Department of Defense
DOI-IBC	Department of the Interior-Interior Business Center
EHR	Electronic Health Record
EIDM	Enterprise Identity Management
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FIT	Financial Innovation and Transformation
FSM	Financial Systems Modernization
FFM	Federal Facilitated Marketplace system
GAO	Government Accountability Office
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HSWL	Health, Safety, and Work life
IEEE	Institute of Electrical and Electronics Engineers

IHiS	Integrated Health Information System
IRS	Internal Revenue Service
IT	Information Technology
ITIM	Information Technology Investment Management Framework
JPMO	Joint Program Management Office
LCCE	Life-Cycle Cost Estimate
PGUI	Provider Graphical User Interface
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SAIC	Science Applications International Corp
SDLC	System Development Life Cycle
SELC	System Engineering Life Cycle
SSA	Social Security Administration
TSA	Transportation Security Administration
UAC	User Applications Component
USCG	United States Coast Guard
USSM	United States Shared Service
VA	Department of Veterans Affairs

EXECUTIVE SUMMARY

Since the creation of the Department of Homeland Security (DHS) in 2002, its components' financial systems have been operating under legacy policies and disparate business processes because of outdated technology. As a result, these systems have been mostly non-integrated or non-interoperable with one another, and many components still rely on manual processes, which have led to inconsistent data and reporting. The United States Coast Guard (USCG) has been the financial service provider for three DHS components: USCG, the Transportation Security Administration (TSA), and the Countering Weapons of Mass Destruction Office (CWMD). These three components—DHS TRIO—exemplify the challenges posed by obsolete financial systems. A new financial management system is therefore needed to fully support Coast Guard financial and acquisition needs and comply with DHS and security requirements. Specifically, the Core Accounting System (CAS)[1] had significant problems such as internal control weaknesses and an inability to produce accurate, reliable, and timely financial information and reports. Likewise, CAS lacked integration with feeder systems such as the Treasury Department, the Office of Management and Budget (OMB), and other USCG inventory and acquisition systems. It thus failed to meet some but not all requirements of the acquisition and financial management community of the USCG. Under these circumstances, the USCG needed to modernize its CAS. This thesis investigates how the USCG can achieve this goal.

The research for this thesis sought to answer the following questions. What can the USCG do to meet the cost and schedule, but more importantly, to increase the likelihood of procuring a system that will meet its financial and operational needs or acquire the value that the agency has paid for? What are the program management processes that USCG needs to develop to make sure the transition to the new financial system can go smoothly?

[1] CAS is the current financial management system for USCG, as well as for the Transportation Security Administration (TSA) and Domestic Nuclear Detection Office which became the Countering Weapons of Mass Destruction office (CWMD) in 2017. It is a highly customized version of Oracle Federal Financials Release ® 11.5.10.

This thesis first includes a comparative analysis of DHS and the USCG's Financial System failure to determine whether this project failure is unique or shares characteristics and challenges with other large government IT projects. Toward this end, the first part of this thesis reviews the lessons learned from DHS TRIO components—USCG, TSA, and CWMD—with the Department of the Interior–Interior Business Center (DOI-IBC) and compares them with other government failures in IT acquisition projects such as HealthCare.gov; the USCG Integrated Health Information System (IHiS); and the Federal Bureau of Investigation's (FBI) virtual case file (VCF). These IT projects share common challenges with the USCG financial system for their relatively large government acquisition programs. Such projects bear inherent risks in terms of their size, interoperability, and integration with different government systems' requirements. Research for this thesis reviewed and identified the similarities that contributed to these large IT acquisition failures. Second, based on the findings of the comparative analysis, this thesis provides recommendations related to both project management and business processes that DHS should apply to successfully transition the USCG and TSA to the new financial management system and the rest of their financial management modernization.

Research for this thesis examined the scholarly debates on the failure of government IT projects. Specifically, it analyzed the scholarly views on causes, risks, and ways to mitigate IT failures. To this end, it reviewed a variety of academic peer-reviewed papers from the Institute of Electrical and Electronics Engineers (IEEE), *Journal of Scientific Research*, *Science Direct*, studies from the Standish Group, Government Accountability Office (GAO) reports, government agencies acquisition life cycle processes and procedures, and articles from *Computerworld* and *Govtech*.

This research found that large government IT projects are often categorized as high risk and likely to fail. They are complex and take longer than two years to develop. Government IT projects are usually built to connect to multiple agencies. These government IT projects affect a wide range of agencies' operational missions and the different type of services that these agencies provide to the public. The four government IT projects this thesis analyzed—DHS TRIO, USCG IHiS, HealthCare.gov, and FBI

VCF—are categorized as large projects.[2] The challenges revealed in the case studies in this thesis are not unique. The initial failures and challenges of the case studies are not isolated cases, and these issues have affected other government projects as well. The case studies and lessons learned in this thesis may contribute to more effective practices that can be used in future big government IT projects.

The four case studies all experienced schedule delays and cost increases. The DHS TRIO and HealthCare.gov projects required significant rework while IHiS and FBI VCF were cancelled and restarted as new projects. The DHS TRIO project costs increased by 54 percent from the original estimate and delayed the delivery schedule by more than two years.[3] The USCG IHiS spent over $56 million; after five years it was cancelled and restarted as a completely new project named DOD MHS GENESIS.[4] The HealthCare.gov cost increased from the original estimate of $292 million to $2.1 billion.[5] The FBI had wasted $105 million by the time the VCF project was cancelled and restarted as a new project in 2005.[6]

The four large government IT projects, DHS TRIO, USCG IHiS, the HealthCare.gov, and FBI VCF, shared similar results. They all experienced significant schedule delays and cost increases, which inevitably led them to fail. The major factors that contributed to the four projects' failures were 1) not defining the project outcomes at

---

[2] The Standish Group, *CHAOS Report: 21st Anniversary Edition* (West Yarmouth, MA: The Standish Group International, Inc., 2014), https://www.standishgroup.com/sample_research_files/CHAOSReport2014.pdf. According to the 2014 Standish report, large IT projects have budgets over $10 million and take over two years to develop, which was the case of all four case studies.

[3] Asif A. Khan, *DHS Financial Management: Improved Use of Best Practices Could Help Manage System Modernization Project Risks*, GAO-17-803T (Washington, DC: Government Accountability Office, 2017), https://www.gao.gov/assets/690/687359.pdf.

[4] David A. Powner, *Coast Guard Health Records: Timely Acquisition of New System Is Critical to Overcoming Challenges with Paper Process*, GAO-18-59 (Washington, DC: Government Accountability Office, 2018), https://www.gao.gov/assets/690/689565.pdf; "MHS GENESIS," Military Health System, accessed April 9, 2021, https://www.health.mil/Military-Health-Topics/Technology/Federal-Electronic-Health-Record-Modernization/MHS-GENESIS.

[5] Alex Wayne, "Obamacare website Costs Exceed $2 Billion, Study Finds," *Bloomberg*, September 24, 2014, https://www.bloomberg.com/news/articles/2014-09-24/obamacare-website-costs-exceed-2-billion-study-finds.

[6] Harry Goldstein, "Who Killed the Virtual Case File? [Case Management Software]," *IEEE Spectrum* 42, no. 9 (September 2005): 24–35, https://doi.org/10.1109/MSPEC.2005.1502526.

the beginning of the Acquisition Life cycle, 2) lacking the right expertise, and 3) having weaknesses in leadership throughout the business process change and the internal control procedures. The projects' challenges and shortcomings led to lessons learned in these four areas for future government and private sector large IT projects.

The four case studies that this thesis reviewed revealed a few important elements that contribute to successful projects, especially government IT projects: defining the project outcomes at the beginning, having the right expertise, leading the organization through the business process change, and fostering internal control procedures.

ACKNOWLEDGMENTS

First and foremost, I wish to express my sincerest appreciation and gratitude to my thesis advisors, Dr. Cristiana Matei and Mr. Jon "Mike" Watson. I would like to thank them for their guidance, their encouragement, and their insightful input. I also would like to thank Mr. Paul Baca, CDR Martin Nossett, and CDR Kevin Beck (USCG) for nominating and endorsing me for the program.

I am incredibly honored to be a part of the Naval Postgraduate School's Center for Homeland Defense and Security program (CHDS). Thank you for teaching me to be a better analyst. I am in awe of the CHDS faculty and staff, Dr. Cristiana Matei, Dr. Chris Bellavita, Mr. Richard Bergin, Dr. Lauren Fernandez, Dr. Shannon Brown, Dr. Nadav Morag, Ms. Lynda Peters, Ms. Greta Marlatt, Ms. Heather Issvoran, Ms. Andrea Page, Mr. Craig Coon, and Mr. Eric Johnsen for their professional contributions and their dedication to the Homeland Security Program.

I also would like to thank Ms. Jasmine Mally. She is the best research and writing coach that anyone could have. I am very grateful for her valuable feedback, her organizational skills, and her kindness.

I am profoundly grateful to my family, my husband, Tung Ly, and my daughter, Fiona Ly, for their unwavering love, support, and patience with me throughout the past years as I spent hours away from them to focus on schoolwork and this thesis. To my sister, my parents, and my extended family who fully supported me and were happy to see me complete the program.

A very special thank you to my mentor and my former supervisor Emeritus Professor Rudy Panholzer. He encouraged me and supported me with my completion of the program. I am forever grateful for his positive impacts on my life.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION: DHS FINANCIAL SYSTEM

A. PROBLEM STATEMENT

Since the creation of the Department of Homeland Security (DHS) in 2002, its components' financial systems have been operating under legacy policies and disparate business processes because of outdated technology. As a result, these systems have been mostly non-integrated or non-interoperable with one another, and many components still rely on manual processes, which have led to inconsistent data and reporting. The United States Coast Guard (USCG) has been the financial service provider for three DHS components: USCG, the Transportation Security Administration (TSA), and the Countering Weapons of Mass Destruction Office (CWMD). These three components—DHS TRIO—exemplify the challenges posed by obsolete financial systems. A new financial management system (FMS) is therefore needed to fully support Coast Guard financial and acquisition needs and comply with DHS and security requirements. Specifically, the Core Accounting System (CAS)[1] has significant problems such as internal control weaknesses and an inability to produce accurate, reliable, and timely financial information and reports. Likewise, CAS lacks integration with feeder systems such as the Treasury Department, the Office of Management and Budget (OMB), and other USCG inventory and acquisition systems. It thus fails to meet some but not all requirements of the acquisition and financial management community of the USCG. Under these circumstances, the USCG needs to modernize its CAS. This thesis investigates how the USCG can achieve this goal.

B. RESEARCH QUESTION

What can the United States Coast Guard do to meet the cost and schedule, but more importantly, to increase the likelihood of procuring a system that will meet its financial and operational needs or acquire the value that the agency has paid for? What are the program

[1] CAS is the current financial management system for USCG, as well as for the Transportation Security Administration (TSA) and Domestic Nuclear Detection Office which became the Countering Weapons of Mass Destruction office (CWMD) in 2017. It is a highly customized version of Oracle Federal Financials Release ® 11.5.10.

management processes that USCG needs to develop to make sure the transition to the new financial system can go smoothly?

In order to answer the main research questions, this thesis also answers these three sub-questions:

1. What are the key characteristics of a large IT investment in government?
2. Why do government IT projects fail?
3. What are some of the risks associated with cost, schedule, and performance in IT acquisition projects?

C. LITERATURE REVIEW

This literature review examines the scholarly debates on the failure of government IT projects. Specifically, it analyzes scholarly views on causes, risks, and ways to mitigate IT failures. To this end, it reviews a variety of academic peer-reviewed papers from the Institute of Electrical and Electronics Engineers (IEEE), *Journal of Scientific Research*, *Science Direct*, studies from the Standish Group, Government Accountability Office (GAO) reports, and articles from Computerworld and Govtech.

A corpus of literature provides insights into the reasons for risks and effects of high failure rates of IT projects. Payne and Anthopoulus et al., for instance, argue that large governmental IT projects seem to fail worldwide because they are complex.[2] Estevez and Joseph, who cite Gauld, Godfinch, Heeks and Scholl have in their article, have all studied government project failures for many years, agreed with Payne and Anthopoulus et al.[3] Similarly, Gil-García and Pardo found that many government IT projects fail because of

[2] Adam Payne, "80% of Major Government Projects Are at 'Risk of Failure' as Civil Servants Struggle to Cope with Brexit," *Business Insider*, January 25, 2018, https://www.businessinsider.com/ifg-report-major-government-projects-at-risk-of-failure-brexit-2018-1; Leonidas Anthopoulos et al., "Why E-Government Projects Fail? An Analysis of the Healthcare.Gov website," *Government Information Quarterly* 33, no. 1 (January 2016): 162, https://doi.org/10.1016/j.giq.2015.07.003.

[3] José Esteves and Rhoda C. Joseph, "A Comprehensive Framework for the Assessment of EGovernment Projects," *Government Information Quarterly* 25, no. 1 (January 2008): 118–32, https://doi.org/10.1016/j.giq.2007.04.009.

their complexity and relatively large scale.[4] They also noted that large projects tend to carry high risk. Furthermore, Yaraghi explained that big government IT projects usually fail not because of inadequate project management but because contractors lack the means or resources to assume that risk, and therefore the government must bear it.[5] Sometimes, as the projects are quite large, both government and contractors fail to accurately estimate project complexity. Likewise, government agencies and contractors set unrealistic expectations for one another that emerge while they are building the system.

Along these lines, the Defense Acquisition Performance Assessment report in 2006 summed up the DOD's failure to estimate the technical complexity and risks of projects, leading to project failure, excessive costs, and delayed completion.[6] The next group of scholars agreed and dove deeper into the root causes of the failure. For example, Fairley and Willshire, as well as Imamoglou and Gozlu, went further and argued that the leading causes of IT project failures are unclearly defined requirements, poor project management, and lack of communication and stakeholder engagement.[7] Several scholars, including Nielsen and Pedersen, as well as Sarantis, Charalabidis and Askounis, agreed with these assessments and further stressed that project management and stakeholder engagement

[4] J. Ramón Gil-García and Theresa A. Pardo, "E-Government Success Factors: Mapping Practical Tools to Theoretical Foundations," *Government Information Quarterly* 22, no. 2 (2005): 187–216, https://doi.org/10.1016/j.giq.2005.02.001.

[5] Niam Yaraghi, "Doomed: Challenges and Solutions to Government IT Projects," *TechTank* (blog), August 25, 2015, https://www.brookings.edu/blog/techtank/2015/08/25/doomed-challenges-and-solutions-to-government-it-projects/.

[6] Ronald Kadish et al., *Defense Acquisition Performance Assessment Report* (Washington, DC: Assessment Panel of the Defense Acquisition Performance Assessment Project, 2006), https://apps.dtic.mil/dtic/tr/fulltext/u2/a459941.pdf.

[7] Richard E. Fairley and Mary Jane Willshire, "Why the Vasa Sank: 10 Problems and Some Antidotes for Software Projects," *IEEE Software* 20, no. 2 (March 2003): 18–25, https://doi.org/10.1109/MS.2003.1184161; Oksan Imamoglu and Sitki Gozlu, "The Sources of Success and Failure of Information Technology Projects: Project Managers' Perspective," in *Technology Management for a Sustainable Economy*, ed. Dundar F. Kocaoglu, Timothy R. Anderson, and Tugrul U. Daim (PICMET '08 - 2008 Portland International Conference on Management of Engineering Technology, Portland OR: IEEE, 2008), 1430–35, https://doi.org/10.1109/PICMET.2008.4599756.

were crucial to the successful execution of a project.[8] Overall, these authors agreed on the importance of setting well-defined requirements to prevent unforeseen complications of the projects later. They highlighted the importance of communication and the involvement of end users or stakeholders. Involving end users or stakeholders can ensure the end product achieves the required process, meets stakeholders' expectations, and makes a positive difference to the end users.

John Marinaro and Benoit Hardy-Vallée also note that IT project failures present high financial and non-financial costs to taxpayers.[9] Indeed, as the OMB notes, in 2019, the United States government spent $83.4 billion on major and non-major IT investment. On the government's online IT dashboard, the federal government posts all IT investment projects and the agencies' Chief Information Officers (CIO) rate risk in their agencies' IT projects based on the criteria set up by the federal government. According to these risk assessments, federal leaders considered 54.2 percent of IT investments to be of medium to high risk before they began.[10] John Marinaro, Vice President of Key Logic, further explains that the assessed high risk reflected the fact that nearly half of all federal employee project managers miss the target by either overspending or failing to fully deliver all the requirements of the projects completed.[11] Government has spent a lot of money to improve the IT infrastructure and strengthen government service programs. However, it has been challenging for government to manage IT programs efficiently and effectively. Many of the projects are too big and high-risk to begin with.

---

[8] Jeppe Agger Nielsen and Keld Pedersen, "IT Portfolio Decision-Making in Local Governments: Rationality, Politics, Intuition and Coincidences," *Government Information Quarterly* 31, no. 3 (July 2014): 411–20, https://doi.org/10.1016/j.giq.2014.04.002; Demetrios Sarantis, Yannis Charalabidis, and Dimitris Askounis, "A Goal-Driven Management Framework for Electronic Government Transformation Projects Implementation," *Government Information Quarterly* 28, no. 1 (January 2011): 117–28, https://doi.org/10.1016/j.giq.2009.10.006.

[9] John Marinaro, "Why Federal IT Projects Fail (and How to Ensure Success)," *Nextgov*, March 11, 2019, https://www.nextgov.com/ideas/2019/03/why-federal-it-projects-fail-and-how-ensure-success/155435/; Benoit Hardy-Vallée, "The Cost of Bad Project Management," *Business Journal*, February 7, 2012, https://news.gallup.com/businessjournal/152429/cost-bad-project-management.aspx?

[10] Office of Management and Budget, "Our Information Technology Investments at Work," *IT Dashboard.gov*, Accessed August 29, 2021, https://myit-2019.itdashboard.gov/.

[11] Marinaro, "Why Federal IT Projects Fail."

The Standish Group has studied IT projects' successes and failures both in the United States and internationally for many years. It agrees with the OMB that large IT projects are high-risk for both government and private sectors.[12] The Standish Group tracked more than 25,000 software development projects in its database from 2003 to 2012 for both government and private sectors that had labor costs of at least $10 million: only 8 percent were successful. As this report noted, 51 percent of the large projects were "challenged," meaning they were over budget, behind schedule, or did not meet the user expectation and the rest of the 41.4 percent were failures. McFarlan's 1981 article "Portfolio Approach to Information Systems" aligns with the Standish Group reports, explaining that there is correlation between larger project size and higher risk in term of failing to meet the anticipated values and staying on budget and schedule. In addition, past Standish Group reports—from 1995, 2001, and 2004—argue that the failed projects were either terminated prior to completion or failed to fulfill the anticipated benefits.[13] As a result, some were morphed into new projects, which would start from scratch.

Similarly, the Federal Bureau of Investigation's (FBI) case management software system, called virtual case file (VCF), utterly failed. The FBI terminated the virtual case initiative after spending about $170 million over four years, starting in 2001, and enduring much scrutiny from Congress and frustration within the agency.[14] By the end of 2004, the FBI concluded that the virtual case initiatives were not going to work.[15] Goldstein explained that the virtual case project was a system, developed by Science Applications

---

[12] The Standish Group, *CHAOS Report: 21st Anniversary Edition* (West Yarmouth, MA: The Standish Group International, Inc., 2014), https://www.standishgroup.com/sample_research_files/CHAOSReport2014.pdf.

[13] F. Warren McFarlan, "Portfolio Approach to Information Systems," *Harvard Business Review* 59, no. 5 (September 1981): 142–50; The Standish Group, *CHAOS Report 1995* (West Yarmouth, MA: The Standish Group International, Inc., 1994), https://www.researchgate.net/publication/263849222; The Standish Group, *Extreme CHAOS* (West Yarmouth, MA: The Standish Group International, Inc., 2001), https://courses.cs.ut.ee/MTAT.03.243/2013_spring/uploads/Main/standish.pdf; and The Standish Group, *CHAOS Report 2004* (West Yarmouth, MA: The Standish Group International, Inc., 2003), http://blog.nalis.fr/public/pdf/q3-spotlight.pdf.

[14] Harry Goldstein, "Who Killed the Virtual Case File? [Case Management Software]," IEEE Spectrum 42, no. 9 (September 2005): 24–35, https://doi.org/10.1109/MSPEC.2005.1502526.

[15] Jerome Israel, "Why the FBI Can't Build a Case Management System," *Computer* 45, no. 6 (June 2012): 73–80, https://doi.org/10.1109/MC.2012.2.

International Corp (SAIC) and the FBI for tracking criminal cases, and further noted that a new project, Sentinel, a $425 million project, replaced the project.[16] Thus, the FBI wasted the funding and efforts invested in the VCF project.

Scholars note that these types of project failures happen in other countries as well. For example, Lohrmann pointed out in 2013 that the National Health Service in the United Kingdom abandoned its massive patient record computer system because the result fell short; the system cost over $16 billion and, if continued, would have cost hundreds of millions of dollars more.[17] The Office of the Auditor General of Canada did an audit on a Canadian IT investment project called the Phoenix pay system. The project, implemented in 2009, was designed to improve the government payroll system to accommodate transactions of up to $22 billion. Instead, the Office of the Auditor General concluded that the Phoenix project failed to meet users' requirements and fixing it would cost the Canadian government millions of tax dollars.[18] In short, large government IT projects, whether in the United States or abroad, come with high risks and have a longstanding history of failing to be completed on time, on budget, and meeting project objectives.

To sum up, many of the scholars and reports above agreed that government IT projects tend to fail or carry a high risk of failure. Many lessons can be learned and improvements can be drawn from these studies.

D. RESEARCH DESIGN

To answer the research question, this thesis includes a comparative analysis of the U.S. Coast Guard's Financial System failure to examine whether this project failure is unique or shares characteristics and challenges with other large government IT projects. Toward this end, the first part of this thesis reviews the lessons learned from DHS TRIO

---

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

17 Dan Lohrmann, "Why Do Many Big IT Projects Fail in Government?," *Lohrmann on Cybersecurity* (blog), November 3, 2013, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/Why-do-many-big-IT-projects-fail-in-government.html.

18 Office of the Auditor General of Canada, *Report 1—Building and Implementing the Phoenix Pay System* (Ottawa, Ontario: Reports of the Auditor General of Canada, May 29, 2018), http://www.oag-bvg.gc.ca/internet/English/att__e_43045.html.

components—USCG, TSA, CWMD—with the Department of the Interior-Interior Business Center (DOI-IBC) and compares them with other government failures in IT acquisition projects such HealthCare.gov, the electronic health care system, and the FBI VCF. These IT projects share common challenges with the U.S. Coast Guard financial system as they are relatively large government acquisition programs. Such projects bear inherent risk in terms of their size, interoperability, and integration with different government systems' requirements. Research for this thesis reviewed and identified the similarities that contributed to these large IT acquisition failures. Second, based on the findings of the comparative analysis, this thesis provides recommendations related to both project management and business processes that DHS should apply to successfully transition the USCG and TSA to the new financial management system and the rest of their financial management modernization.

E. THESIS OVERVIEW

Chapter II presents the case studies of DHS TRIO Financial Management Modernization project. Chapters III, IV, and V review other unsuccessful acquisition projects such as the USCG Integrated Health Information System (IHiS), HealthCare.gov, and the FBI virtual case management project. Chapter VI presents the findings from the research, recommends uses for the findings, and identifies areas for further study.

THIS PAGE INTENTIONALLY LEFT BLANK

II. EVALUATING THE DHS TRIO PROJECT

In 2016, more than two years into the agreement between DHS and DOI-IBC, many issues arose related to costs, technical requirements, and schedule. GAO conducted a review on the DHS Financial Management TRIO acquisition project that revealed many problems with the program's cost and delivery schedule. For example, the estimated cost for the TRIO project increased by 54 percent from the original estimate because of an increase in project requirements, lack of expertise, lack of leadership, and failure in business process change.[19] As noted in the hearing before the subcommittee on oversight and management efficiency, DOI-IBC could not fully meet the technical requirements of TRIO. In addition, DOI-IBC struggled to grasp the complexity of the TRIO project; DOI-IBC had never provided financial services to a large agency like DHS.[20] DHS realized that DOI-IBC would not be able to deliver the financial systems originally intended for the TSA and USCG. In February 2017, DHS notified the congressional Committee on Homeland Security that the TRIO financial management system modernization project with DOI-IBC had generated cost overruns and breached the delivery schedule.[21] After more than three years of partnership and configuration efforts, DHS cancelled the contract with DOI-IBC in May 2017.

This chapter first gives background on a key element of acquisition programs, the analysis of alternatives (AoA). TRIO's implementation of the AoA was one of its key weaknesses in the execution of the acquisition, which is described in detail in the project requirements and scope section. The review also focuses on whether the TRIO project had

---

[19] Asif A. Khan, *DHS Financial Management: Improved Use of Best Practices Could Help Manage System Modernization Project Risks*, GAO-17-803T (Washington, DC: Government Accountability Office, 2017), https://www.gao.gov/assets/690/687359.pdf, 8.

[20] DHS Financial Systems: Will Modernization Ever Be Achieved? Hearing Before the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives, 115th Cong. 1 (2017), https://www.govinfo.gov/content/pkg/CHRG-115hhrg28418/pdf/CHRG-115hhrg28418.pdf.

[21] Charles D. Michel, ADM, "Financial Management Service Improvement Initiative (FMSII) Program Breach Notification" (official memorandum, Washington, DC: United States Coast Guard, 2017).

the right leadership and expertise for the project and how well leadership managed the business changes.

A. ANALYSIS OF ALTERNATIVES

The DHS Acquisition Life cycle framework includes four major acquisition phases (Figure 1):

1. Need: identifies the need or operational gaps and the need for a system that would fulfill operational mission;
2. Analyze/Select: analyzes alternative solutions to reach a decision on the optimal solution (material and/or non-material) that will address the problem;
3. Obtain: develops or obtains a chosen material solution;
4. Produce Deploy Support: produces, deploys, and supports the solution in its operational environment and disposes of the system at the end of its life cycle.

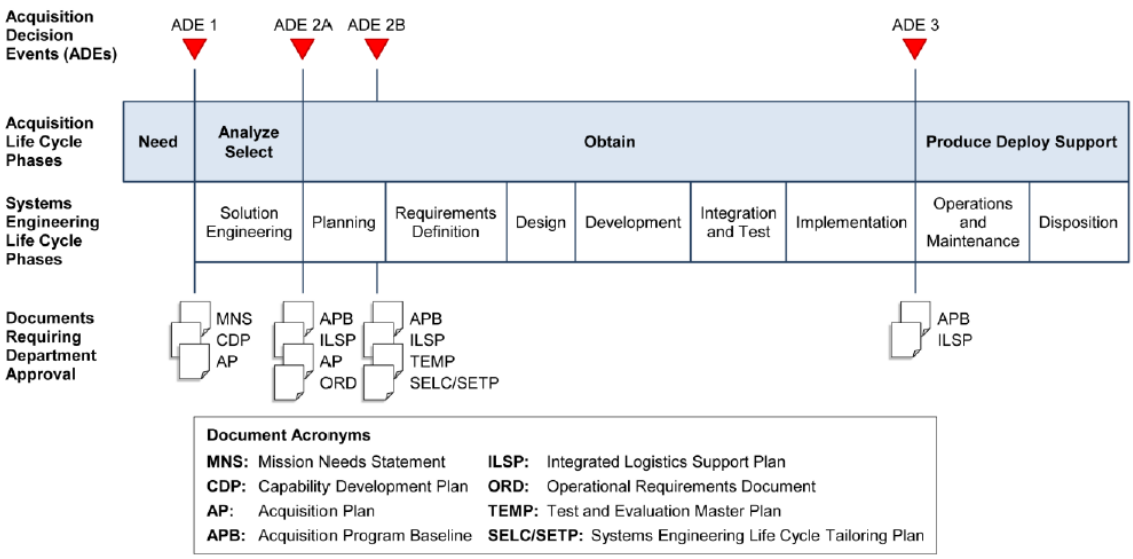

Figure 1. DHS Acquisition Life Cycle.[22]

The AoA is conducted early in the acquisition process to identify trade-offs between alternatives to come up with the best solution; it spans from the Need phase to the Analyze/Select phase in the DHS Acquisition Life cycle. The main objectives of a typical AoA are to document a needed system and concept of operations, define the metrics, and identify alternative products or services. An AoA is designed to meet the project's needs, analyze cost, and evaluate risks, performance, operational effectiveness and trade-offs among cost and needed capabilities. Figure 2 shows the major steps of analysis in the AoA process.

[22] Bryant Streett, *Analysis of Alternatives (AoA) Methodologies: Considerations for DHS Acquisition Analyses, Version 3.0*, RP13-01.04.05-01 (Falls Church, VA: Homeland Security Studies and Analysis Institute, 2014), https://www.anser.org/docs/reports/AOA%20Methodologies%20Considerations%20for%20DHS%20Acq%20Analysis.pdf.

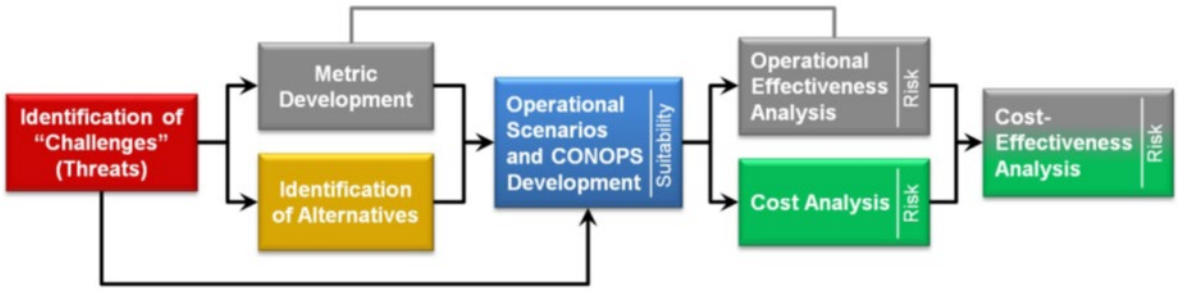

Figure 2. Typical Phases of an AoA[23]

A typical AoA takes, on average, over a year to complete and it includes seven steps. The AoA first identifies "challenges" (or threats) and develops a concept of operations (CONOPS); these processes happen in the first phase of the DHS Acquisition Life cycle, the Need phase. A gap analysis helps the organization identify what is missing in their capability to meet the current threats or operational requirements. The CONOPS outlines how the new financial system will help USCG and DHS operation and how it ties to DHS missions.

After the challenges and CONOPS have been clearly defined, the AoA proceeds to metric development and identification of alternatives. The metric development process defines the performance measurements tied to the operational mission. Within the identification of alternatives step, market research is usually conducted to determine the availability and suitability of products and services. After identifying possible products that meet the project's requirements, the AoA proceeds to analyze operational effectiveness and cost. The cost-effectiveness analysis calculates cost by evaluating the possible systems' operational performance given the risks and constraints. The cost-benefit analysis simply weighs all the risks against the possible solutions at different cost levels to recommend the best service based on the level of funding available. OMB Circular A-94 defines program cost-effectiveness analysis as a quantitative method for comparing the cost of alternatives in order to select the lowest cost, with inflation included, for a given amount of benefits.[24]

[23] Streett, Analysis of Alternatives, 9.

[24] Office of Management and Budget, *Guidelines and Discount Rates for Benefits-Cost Analysis of Federal Programs*, OMB Circular A-94 (Washington, DC: Office of Management and Budget), 5, accessed April 23, 2021, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A94/a094.pdf.

However, the circular guidance encourages government agencies to perform cost-benefit analysis when considering different alternatives by holistically applying cost, policies and long-term effects on the government program.[25]

David Trimble documented the best practices for an AoA in a 2014 GAO report. The report explains that identifying mission need or how the new acquired system would benefit the organization is the first requirement in the best practices for the AoA process.[26] In addition, the AoA must include all the methodologies and assumptions used in the analysis. Most importantly, the mission need and analysis in the AoA needs to be done without a predetermined solution.

B. PROJECT REQUIREMENTS AND SCOPE

During the first year DHS worked with DOI-IBC, from October 2013 to May 2014, the USCG identified numerous functional and technical requirements, reports, interfaces, and other complexities associated with transitioning to a new financial management program. Additional requirements, such as how the financial system should interface with human resources, procurement, and other asset systems such as aviation, and naval surface logistic systems, made the financial modernization more complicated. The USCG has many assets such as National Security Cutters, High Endurance Cutters, Fast Response Cutters, different types of small boats, in addition to helicopters MH-60 and MH-65, and airplanes C-27J and C-130.[27] Each asset serves multiple missions that tie to DHS's "six strategic missions and five non-homeland security missions."[28] It was challenging for DOI-IBC to support the transition of a big agency like the Coast Guard to a new financial system that required capabilities both to capture all current and future financial report needs and also to comply with all updated cyber security requirements.

---

[25] Office of Management and Budget, 18.

[26] David C. Trimble, *DOE and NNSA Project Management: Analysis of Alternatives Could Be Improved by Incorporating Best Practices*, GAO-16-37 (Washington, DC: Government Accountability Office, 2014), 44–45, https://www.gao.gov/assets/670/667404.pdf.

[27] "Coast Guard Operational Assets," United States Coast Guard, accessed April 30, 2021, https://www.uscg.mil/About/Assets/.

[28] "Missions," United States Coast Guard, accessed April 30, 2021, https://www.uscg.mil/About/Missions/.

In testimony to the Committee on Homeland Security on Sep 26, 2017, DHS, TRIO and IBC representatives all agreed that lack of understanding of the complexity of the TRIO project requirement early in the Acquisition Life cycle affected DHS's and IBC's ability to complete the TRIO project on time.[29] Such complexities had not been accounted for during the Analyze/Select acquisition phase market research in the 2013 AoA.[30] Because the phases of the Acquisition Life cycle are cumulative, poor execution of the early phases negatively impacts the subsequent ones. The extensive report on the DHS TRIO project published on September 26, 2017 documented that the project inadequately executed the AoA in the pre-acquisition phase.

One major deficiency in TRIO's AoA stemmed from not establishing a CONOPS during the Need phase. TRIO did not realize the one alternative it identified—DOI-IBC's financial management services—would not meet all its needs, as TRIO failed to develop a CONOPS at the appropriate time. According to Asif Khan's 2017 GAO report, the mission statement or CONOPS for the financial management project for USCG was supposed to be included as a part of the AoA, but the report found that the CONOPS was done after completion of the AoA.[31] Before an acquisition project starts, the mission needs a statement of how the new project will support a government agency operation, which must occur in the pre-acquisition phase. In the absence of a CONOPS, the GAO report did not indicate what DHS used to help judge the suitability of the service they chose to acquire—those of DOI-IBC.

Another significant error that occurred during the pre-acquisition phases was that TRIO failed to analyze alternatives. The only service considered was a government shared service through DOI-IBC. The testimony indicated the TRIO project followed OMB guidance.[32] OMB Memorandum M-13-08 directed executive agencies to use a federal

---

[29] Khan, DHS Financial Management: Improved Use, 9.

[30] Asif A. Khan, *DHS Financial Management: Better Use of Best Practices Could Help Management System Modernization Project Risk*, GAO-17-799 (Washington, DC: Government Accountability Office, 2017), https://www.gao.gov/assets/690/687362.pdf.

[31] Khan.

[32] H.R., DHS Financial Systems.

shared service—which is a service that one branch or agency of government provides to other branches or agencies of government—for modernizing their future financial management system when it is available.[33] Using a shared service is designed to promote efficiency and eliminate duplication across government.[34] The DHS TRIO Project limited its market research because DHS did not consider other alternatives outside the government. It only considered federal shared services under the guidance of this OMB memorandum. As a result, TRIO failed to evaluate which systems were available in the private sector to meet the technical requirements. Likewise, collectively, TRIO failed to account for the trade-offs between effectiveness and cost for each available option.[35] Contrary to AoA best practices, TRIO came into the AoA process with a predetermined solution, which was a federal shared service.

TRIO also failed to thoroughly document risk assessment and risk mitigation strategies for technical risk and other risks such as cost and schedule. Figure 2 shows the typical risk analysis that should be conducted in an AoA before the service is selected to document major risks and how to mitigate those risks for each alternative.[36] Acquisition programs then rank risks based on their impact on mission needs and functional requirements. All risks "are documented for each alternative along with any overarching or alternative specific mitigation strategies."[37] However, without a CONOPS, technical risk cannot be adequately measured. The CONOPS would have given TRIO a chance to do a better evaluation of the effectiveness of the new financial management system service to benefit DHS operational missions. This initial analysis could have also revealed that the

[33] Danny Werfel, "Improving Financial Systems through Shared Services," M-13-08 (Memorandum for the heads of executive departments and agencies, Washington, DC: Office of Management of Budget, March 25, 2013), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2013/m-13-08.pdf; Khan, *DHS Financial Management: Better Use*, 5.

[34] "Shared Services," General Services Administration, accessed April 9, 2021, https://www.gsa.gov/shared-services.

[35] Khan, DHS Financial Management: Better Use, 16.

[36] Marie A. Mark, Amphibious Combat Vehicle: Some Acquisition Activities Demonstrate Best Practices; Attainment of Amphibious Capability to Be Determined, GAO-16-22 (Washington, DC: Government Accountability Office, 2015), https://www.gao.gov/assets/gao-16-22.pdf.

[37] Mark.

service would need substantial upgrades to meet TRIO's needs. Identifying the system requirements after the AoA was completed hindered an effective technical analysis.

Beyond the technical risks, all acquisition programs should also examine schedule and cost risks. TRIO had not documented cost and schedule risks as of July 2016, during the Obtain phase.[38] TRIO did attempt a life-cycle cost estimate (LCCE) but did not do a thorough job. TRIO used the estimate from the service provider, DOI-IBC, instead of developing an LCCE on its own.[39] After obtaining this cost estimate, the USCG failed to independently validate it.[40] In the testimony, the USCG/TRIO did not explain its LCCE process or why it failed to complete this requirement correctly. However, the GAO report did indicate that the cost estimates relied on rough estimates, not on work broken down by structure or level.[41] A more detailed analysis would have given a more accurate cost estimate. According to Tim Persons' *Cost Estimating and Assessment Guide*, cost estimate should be well documented, all assumptions should be independently verified by a group other than cost estimators, and the estimate should be done by government not vendors.[42] In addition, the cost estimate should include adjusted inflation to capture the total cost and all the assumptions should be thoroughly documented so that auditors can replicate the cost estimate following the documented assumptions and processes.[43] However, for the TRIO project, neither the USCG nor DOI-IBC applied net present value in the life cycle cost estimate. Furthermore, the cost estimate was done mostly by DOI-IBC in a manner that did not reflect best practices for cost estimate**.** Therefore, the original cost estimate for the TRIO project in 2013 and 2014 in the AoA was much lower than the actual cost of the project. Risk is included in the AoA and is inherently a part of every alternative in the AoA

[38] Khan, DHS Financial Management: Better Use, 24.

[39] Khan.

[40] Khan.

[41] Khan.

[42] Timothy M. Persons, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, GAO-20-195G (Washington, DC: Government Accountability Office, 2020), https://www.gao.gov/assets/gao-20-195g.pdf.

[43] Persons, 191–200.

process, yet TRIO's lack of risk analysis resulted in unknowingly selecting a service provider with a high amount of risk, which contributed to the failure of the project.

At the congressional hearing on DHS financial project in September 2017, DHS, DOI-IBC, the Office of the Financial Innovation and Transformation under Department of Interior (FIT) that oversees the federal shared service provider, and United States Shared Service (USSM) GSA all agreed on why the TRIO project failed.[44] They noted that inability to grasp the full scope and complexity of the requirements of the DHS financial modernization project in its early phase affected the DOI-IBC and DHS's ability to complete the financial management system as planned.[45] During the first phase of the acquisition process, the TRIO project collectively failed to meet the benchmarks established in the AoA's best practices. The TRIO project only partially met some of the AoA recommended practices (i.e., that each process should be well documented, comprehensive, unbiased, and credible).[46] Table 1 is GAO's evaluation of DHS TRIO Components' AoA. It shows that both the USCG and TSA did not substantially meet the requirements for a reliable and high-quality AoA. Without a proper AoA and clearly defined requirements, TRIO failed to evaluate how the new financial system would support the DHS mission and the full scope of its total cost from development to software operation.

[44] Khan, DHS Financial Management: Better Use.

[45] Khan.

[46] Asif A. Khan, *DHS Financial Management Improved Use of Best Practices Could Help Manage System Modernization Project Risks,* Testimony Before the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives, GAO-17-803T (Washington, DC: Government Accountability Office, 2009).

Table 1. DHS TRIO Components' Adherence to Characteristics of a Reliable, High-Quality Analysis of Alternatives Process.[47]

	Overall GAO assessment[a]		
AOA characteristic	**Coast Guard**	**TSA**	**DNDO**
Well-documented: The analysis of alternatives (AOA) process is thoroughly described, including all source data, clearly detailed methodologies, calculations, and results, and selection criteria are explained.	Average score: 3.25 Partially met	Average score: 3.25 Partially met	Average score: 3.5 Substantially met
Comprehensive: The level of detail for the AOA process ensures that no alternatives are omitted and that each alternative is examined thoroughly for the project's entire life cycle.	Average score: 3.6 Substantially met	Average score: 3.4 Partially met	Average score: 3.8 Substantially met
Unbiased: The AOA process does not have a predisposition toward one alternative over another but is based on traceable and verified information.	Average score: 3.0 Partially met	Average score: 3.43 Partially met	Average score: 4.0 Substantially met
Credible: The AOA process discusses any limitations of the analysis resulting from the uncertainty surrounding the data to assumptions made for each alternative.	Average score: 3.33 Partially met	Average score: 3.5 Substantially met	Average score: 3.83 Substantially met

C. LEADERSHIP AND EXPERTISE

During the Obtain phase, DOI-IBC noted that they did not have the right resources and expertise in engineering and information technology, and that they suffered from high staff turnover that hindered the success of the project. In the subcommittee hearing in the House of Representatives, DHS and DOI-IBC officials stated that DOI-IBC had experienced many challenges with hiring federal employees and DOI-IBC was not able to hire the right expertise in time to meet the required deliverables for TRIO's project. In addition, DOI-IBC experienced high turnover in key leadership and in positions that supported the TRIO project.[48] In sum, DOI-IBC did not have the experienced staff to fulfill a large-scale and complex project like the TRIO.

Another complication to the TRIO project was that it required significant customization to meet DHS's six overarching operational missions and provide the ability to capture expenditures for each mission. Software customization is not recommended by J. R. Blanchette because the modifications to fit the customer's needs are not part of the vendor's

[47] Khan, DHS Financial Management: Better Use.

[48] H.R., DHS Financial Systems, 28.

line of product.[49] Blanchette explains that customization may deviate from the vendor expertise and could result in unsuccessful software implementation or issues with maintenance later. In addition, under the shared service model in OMB Circular A-127, government agency customers usually request a service that the provider agency understands quite well and currently provides via software or system to existing customers.[50] However, TRIO requested a newer version of the Oracle Federal Financial software (version 12.2), and DOI-IBC staff was unfamiliar with this version, as the September 2017 GAO 17–803T report found.[51] Thus, on the one hand, DHS deviated from the regular business of government shared services. On the other hand, incorporating Oracle 12.2 version in 2014—which differed greatly from Oracle version 11.1 that DOI-IBC employed at the time—greatly increased the complexity of the project. As a result, the DOI-IBC lacked the necessary expertise to customize the system and meet the TRIO project's needs.

The GAO further found that DHS did not apply the concept of earned value management to the financial management project with DOI-IBC to the fullest extent necessary for effective acquisition management.[52] The earned value management tool focuses on the combination of cost, schedule, technical process, and risk. Earned value management is often used as a measurement tool for acquisition program managers to assess acquisition progress to determine whether the programs meet schedule or budget. During testimony, a DHS official promised Congress that DHS would require earned value management from the next selected vendors for TRIO to ensure the quality for the project.[53]

Moreover, the TRIO program lacked a communication strategy to dictate how the three DHS components—CWMD, TSA, and USCG—were to communicate with each other

---

[49] J. R. Blanchette, "Pros and Cons of Using COTS Products," in *IEEE Autotestcon 2005* (conference proceedings), (Orlando, FL: IEEE, 2005), 472–476, doi: 10.1109/AUTEST.2005.1609182.

[50] Office of Management and Budget, *Financial Management Systems*, interim final revision of OMB Circular A-127 (Washington, DC: Office of Management and Budget, 1999). https://www.whitehouse.gov/wp-content/uploads/2017/11/Interim-Final-Revision-of-OMB-Circular-A-125-July11999.pdf.

[51] Khan, DHS Financial Management: Improved Use.

[52] Persons, *Cost Estimating and Assessment Guide*, 219. Earned Value Management is an acquisition management tool. It measures the value of actual work accomplished and compares it with the value of planned of value of work in a given period of time.

[53] H.R., DHS Financial Systems.

and with DOI-IBC. The TRIO program was not centrally managed during the acquisition process with DOI-IBC.[54] The oversight of the TRIO program was split across the three DHS components. In the testimony to the Committee on Homeland Security, Mr. Chip Fulghum, a DHS official at the time, told the committee that "communication between TRIO and IBC was not cohesive, and was not well coordinated."[55]As a result, it was challenging for both TRIO and DOI-IBC to collaborate for the new financial management system. The weak communication channel between TRIO and DOI-IBC caused difficulty in decision-making processes for any system changes during the acquisition processes.[56]

D. BUSINESS PROCESS CHANGE

Business process change includes change in management, change in management communication, the buy-in process (which involves end users), and the process of developing a new manual and training—which all occur in the Obtain phase of the DHS Acquisition Life cycle. Business process change is crucial for any acquisition program to be implemented successfully. When an organization implements a new system, it usually causes changes in day-to-day operations. Therefore, business process change involved the organizations' changes, and the workforce's changes to adapt to the new acquisition system. However, business process change must tie back to the architecture enterprise or how the new acquisition is to benefit and fit into the organization's operational missions in the Need phase. Based on the congressional testimony in September 2017 and the two GAO reports that analyzed the failure of the TRIO project with DOI-IBC, DHS agreed that DHS had failed to prepare for change management by not involving all the stakeholders in the buy-in process and not helping the stakeholders understand how the new system would operate.[57]

The TRIO project team focused on the delivery of the software and did not pay enough attention to change management.[58] Consequently, the agency was not ready for the

[54] Khan, DHS Financial Management: Improved Use, 13–16.

[55] Khan, DHS Financial Management: Improved Use.

[56] Khan, 33,45-47.

[57] Khan, 8.

[58] Khan, DHS Financial Management: Better Use.

new financial management system. According to the Project Management Institute, the practice of change management is an inclusive, collaborative, "structured approach for transitioning individuals, groups, and organizations from a current state to a future state with intended business benefits or positive future outcomes."[59] Change management brings organizations, individuals, process and strategy together to collaborate toward a new process or new system. However, TRIO failed to take the program through an effective organizational change management process to transition to a new financial management system. Therefore, the TRIO failed many steps in the business process change.

E. CONCLUSION

The project moved forward despite the inadequate application of the steps in the pre-acquisition phase, resulting in problems transitioning to the new financial system. The poor AoA execution resulted in poor definition of the project's requirements and scope. Consequently, the DHS project required significant customization to meet agency operational needs. The fact that TRIO did not clearly define a CONOPS and did not document the risks and related mitigation strategies for the service it selected—when it should have also examined various alternatives—prevented DHS decision makers from performing a meaningful analysis necessary to balance between time and cost. This misstep prevented DHS from choosing a recommended alternative: regular commercial vendor, government shared service, or commercial shared service. In sum, TRIO established the project's requirements during the Need and Analyze Select phases but failed to complete the AoA process and the CONOPS at the appropriate time. It also had weak leadership and project management, and failed to implement business process change. All of these factors contributed to the discontinuation of the TRIO project with DOI-IBC. DOI-IBC completed most of the implementation for the CWMD financial system, but TSA and USCG had to change to another commercial vendor for their financial modernization effort.

---

[59] J. Christopher Mihm and Robert Goldenkoff, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, DC: Government Accountability Office, 2018), 5–6, https://www.gao.gov/assets/gao-18-427.pdf; Project Management Institute, Inc., *Managing Change in Organizations: A Practice Guide* (Newtown Square, PA: Project Management Institute, Inc., 2013), 19.

The TRIO program has taken steps to avoid further problems and to ensure the possibly of project success. Accordingly, in July 2017, the DHS Acquisition Review Board cancelled the TRIO project with DOI-IBC. Since the discontinuation of the TRIO project, DHS derived many lessons learned and applied them to the agency's continuing financial system modernization efforts. During the hearing on September 26, 2017, DHS official Mr. Chip Fulghum said that DHS had taken lessons learned from the DOI-IBC engagement. DHS was more prepared to support the initiative going forward: "DHS has changed its implementation approach from individual component projects to a centralized DHS initiative."[60] The TRIO program has since added a Joint Program Management Office (JPMO). The JPMO has provided centralized program governance and streamlined decision making since the termination with DOI-IBC. Since 2017, the TRIO project has been administered within the newly formed Office of the Chief Financial Officer (OCFO), managed by the DHS Financial Systems Modernization JPMO[61] with CWMD, TSA, and USCG engagement.

In December 2017, the DHS Office of Procurement Operations awarded a System Deployment Agent support services contract to the IBM Corporation.[62] IBM is currently the commercial shared service provider/contractor for the DHS TRIO project. Although CWMD completed the transition to a new financial system in October 2019, TSA and the USCG implementation have been delayed to FY21 and FY22.[63] The DHS TRIO project remains in the Obtain DHS acquisition phase.

---

[60] Khan, DHS Financial Management: Improved Use, 42–47.

[61] Khan, DHS Financial Management: Improved Use.

[62] U.S. Coast Guard, "ALCOAST 091/18 - Mar 2018 Financial Management and Procurement Services Modernization - Update 2," U.S. Coast Guard, March 14, 2018, https://content.govdelivery.com/accounts/USDHSCG/bulletins/1e206d1.

[63] Khan, DHS Financial Management: Better Use.

III. USCG HEALTH CARE PROJECT

The second case study also falls within the DHS and covers the Coast Guard's efforts to modernize its electronic health care system. Coast Guard Health Care services support 41 Coast Guard base clinics and 125 medical facilities afloat and ashore that treat over 50,000 active-duty members.[64] In 2002, the Coast Guard implemented a Department of Defense (DOD) Composite Health Care System (CHCS) for medical record services including scheduling patient appointments and keeping medical records such as prescriptions and referrals. Furthermore, CHCS interoperated with other DOD health care systems such as prescription repositories, labs, and the military health insurance system.[65] In addition to implementing the CHCS, in 2004 the Coast Guard added another DOD system, the Provider Graphical User Interface (PGUI) to the health care system modernization effort. PGUI was an enhanced support system of CHCS intended for creating and keeping medical notes electronically.

However, both the PGUI and CHCS systems lacked the capability to bill, schedule, and support case management. As a result, in 2009, the Coast Guard changed its modernization plan and set the intention to transition its medical system to a more modern system run by the DOD, called the Armed Forces Health Longitudinal Technology Application (AHLTA).[66] Nevertheless, as noted by Coast Guard Health, Safety and Work Life (HSWL) in the GAO 18–59 report, once again, the Coast Guard changed its modernization plan in 2010 for two reasons: 1) the Coast Guard's mission requirements differ from the DOD's; and 2) the DOD's modernization of its health care system—AHLTA—was too expensive, so the Coast Guard decided to acquire its own medical

64 David A. Powner, *Coast Guard Health Records: Timely Acquisition of New System Is Critical to Overcoming Challenges with Paper Process*, GAO-18-59 (Washington, DC: Government Accountability Office, 2018), https://www.gao.gov/assets/690/689565.pdf, 5.

65 Powner, Coast Guard Health Records.

66 Powner.

system. The Coast Guard's new health care system was to be designed to interface with the DOD and the Department of Veterans Affairs (VA).[67]

The Coast Guard awarded $14 million and a five-year contract to obtain an electronic health record (EHR) system from commercial vendors in September 2010. The new health care system was a commercial-off-the-shelf (COTS) system that provided outpatient services including online schedules and patient records. The scope of the new health service system expanded beyond EHR modernization to include other services, and the name changed to the Integrated Health Information System (IHiS) project. The project cost total in 2010 was estimated at around $56 million, which included the initial cost of $14 million according to GAO-18-59 report.[68] USCG contracted over 25 different vendors including Epic, Leidos, and other companies to support the IHiS project.[69]

The new health care system under the IHiS project was to be implemented in phases with a few Coast Guard clinics in October 2015, and then at the other clinics, sick bays, and for Department of State locations. However, after five years into the Obtain phase and spending nearly $60 million on the project, the Coast Guard decided to cancel the IHiS project in October 2015.[70] The IHiS issues such as cost, schedule and technical complexities were listed as the main reasons the Coast Guard canceled the project.[71] The acquisition project resulted neither in useable software nor in any tangible assets to support the health care system in the future.[72]

This chapter reviews how well the program defined the project requirements and managed the project. The review also focuses on whether the IHiS project had the right

---

67 Powner.

68 Powner.

69 Arthur Allen, "Coast Guard Docs Return to the Age of Paper," *Politico Morning EHealth* (blog), April 22, 2016, https://www.politico.com/tipsheets/morning-ehealth/2016/04/coast-guard-docs-return-to-the-age-of-paper-hhs-cyber-task-force-underway-213914.

70 Powner, Coast Guard Health Records.

71 Powner.

72 Carol C. Harris, Information Technology: Implementation of GAO Recommendations Would Strengthen Federal Agencies' Acquisitions, Operations, and Cybersecurity Efforts, GAO-19-641T (Washington, DC: Government Accountability Office, 2019), https://www.gao.gov/products/GAO-19-641T.

leadership and expertise for the project and how well leadership managed the business changes.

A. PROJECT REQUIREMENTS AND SCOPE

To evaluate the USCG health system modernization effort, this section reviews the IHiS project from project requirement and scope perspectives by reviewing how well the IHiS project applied the principles and guidance in the Acquisition Life cycle, especially in the Need and Analyze/ Select Phases. This section first describes the System Development Life Cycle (SDLC), the process the USCG stated it used to acquire the system. Then, the section reviews how the USCG applied the SDLC process for IHiS.

1. System Development Life Cycle

The USCG followed the non-major acquisition program and SDLC process developed by the CIO, office of the Assistant Commandant for C4&IT for the IHiS project.[73] SDLC is the USCG Commandant's instruction for developing an IT system from conceptual planning through design, development, testing, operation and maintenance and disposition.[74] At the time of the IHiS acquisition project, non-major acquisition programs followed the SDLC process while major systems acquisition programs followed the major system acquisition manual and the System Engineering Life Cycle (SELC).[75] The Coast Guard SDLC defines non-major acquisition programs as a those with acquisition budgets

---

[73] U.S. Coast Guard, *USCG System Development Life Cycle (SDLC) Practice Manual, Revision 4.0*, SDLC Product #107 (Washington, DC: U.S. Coast Guard, 2011), https://cg.portal.uscg.mil/communities/sdlc--pprb--pprb-wg/SDLC/LIBRARY/PRODUCTS/PRACTICE/Current%20Final.pdf.

[74] "Electronic Health Records Acquisition," U.S. Coast Guard Acquisition Directorate, accessed August 24, 2020, https://www.dcms.uscg.mil/Our-Organization/Assistant-Commandant-for-Acquisitions-CG-9/Programs/C4ISR-Programs/Electronic-Health-Records-Acquisition/.

[75] United States Coast Guard, *LEVEL 3 NON-MAJOR ACQUISITION PROGRAM (NMAP) MANUAL*, COMDTCHANGENOTE 5000, COMDTINST M5000.11C, 2019, https://media.defense.gov/2019/Jun/12/2002144388/-1/-1/0/CIM_5000_11C.PDF; United States Coast Guard, *Major Systems Acquisition Manual (MSAM)*, COMDTINST M5000, COMDTINST M5000.10A Version 2.1 (Washington, DC: Department of Homeland Security, 2009), https://www.hsdl.org/?view&did=22315; U.S. Coast Guard, *System Development Life Cycle (SDLC)*, SDLC Practice Manual #107 (Washington, DC: U.S. Coast Guard, 2011), https://cg.portal.uscg.mil/communities/sdlc--pprb--pprb-wg/SDLC/LIBRARY/PRODUCTS/PRACTICE/Current%20Final.pdf; David A. Powner, *Coast Guard Health Records: Timely Acquisition of New System Is Critical to Overcoming Challenges with Paper Process*, GAO-18-59 (Washington, DC: Government Accountability Office, 2018), https://www.gao.gov/assets/690/689565.pdf.

under $300 million for the entire life cycle, from the Need phase to the Produce/Deploy/ Support/Dispose phase.[76] At this time, SELC is mandated for all acquisition programs. As of 2019, the USCG has updated all major and non-major acquisition projects to use the SELC to comply with DHS Acquisition Instruction 102–01-001,[77] which provides guidelines for the Acquisition Life cycle, instead of following the previous procedure, SDLC.

The SDLC is a business engineering process embedded in the Acquisition Life cycle. Figure 3 compares the USCG acquisition decision events (ADEs) and Phases for Non-Major Acquisition Programs with the SDLC process. The USCG Acquisition Life cycle Framework in Figure 3 is represented by the top four boxes: Need phase, Analyze/ Select phase, Obtain phase, and the Produce/Deploy/Support/Dispose phase. There are seven phases in the SDLC process within the four phases of the Acquisition Life cycle: 1) conceptual planning 2) planning requirements, 3) design, 4) development and testing 5) implementation, 6) operational and maintenance, and 7) disposition[78]—the yellow blocks in Figure 3. The USCG's explanation of the main processes in the seven phases of the SDLC is summarized in Table 2.

[76] U.S. Coast Guard, System Development Life Cycle Practice Manual, 28.

[77] U.S. Coast Guard Acquisition Directorate, *Level 3 Non-Major Acquisition Program (NMAP) Manual*, COMDTINST M5000.11C, (Washington, DC: U.S. Coast Guard Acquisition Directorate, 2019) https://media.defense.gov/2019/Jun/12/2002144388/-1/-1/0/CIM_5000_11C.PDF; U.S. Coast Guard Acquisition Directorate, *Major Systems Acquisition Manual (MSAM)*, COMDTINST M5000.10A Version 2.1 (Washington, DC: U.S. Coast Guard Acquisition Directorate, 2009), 57, https://www.hsdl.org/?view&did=22315.

[78] U.S. Coast Guard, System Development Life Cycle Practice Manual, 24.

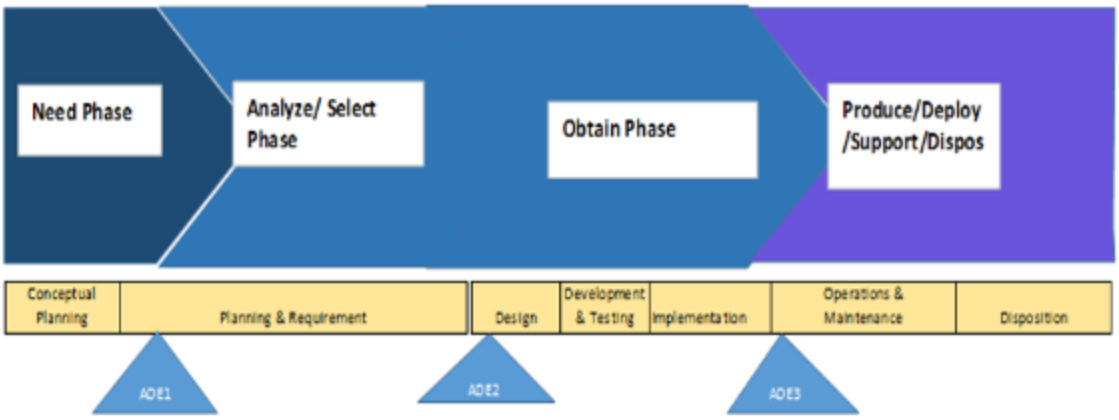

Figure 3. USCG Acquisition Life Cycle Framework with Acquisition Decision Event For Non-Major Acquisition Program.[79]

Table 2. USCG System Development Life Cycle[80]

Review	Purpose
1. Conceptual Planning Phase	Program is supposed to validate the requirements of the acquisition program to meet the overall organization's operational mission, also known as the enterprise architecture. Program also formalizes the roles and responsibilities, such as the project manager, asset manager, and establishing committees that provide the oversights for the program.
2. Planning and Requirement Phase	Program establishes a project plan including cost, estimate, work breakdown structure, risk management, and life cycle cost estimate.
3. Design Phase	Program develops the detailed system design to specify the operating system, architecture components, developing the operational analysis plan to document system measurement for reliability, maintainability and availability. This phase also covers training for the users, obtaining users inputs and enhancing user buy-in.
4. Development and Testing Phase	Testing happens in this phase. Users participate in testing to validate the system to meet the organization objectives and the users' needs.
5. Implementation	The new system obtains the approval for operation in the production environment. The program office coordinates training.

[79] Adapted from U.S. Coast Guard System Development Life Cycle, 20; Powner, Coast Guard Health Records, 34.

[80] Adapted from U.S. Coast Guard, System Development Life Cycle Practice Manual.

Review	Purpose
6. Operations and Maintenance	The new acquisition system operates according to the specification and the program office continue to make sure the new system meets the organization's and users' needs. User training continues to happen in this process. User support continues.
7. Disposition	This process is at the end of the system life cycle. It ensures that the system is disposed in accordance with law and regulations.

In addition to these seven phases of the SDLC, there are three ADEs that every non-major acquisition program has to complete before moving to the next phase. An ADE is an important check and balance tool in the acquisition framework. In order for a program to receive approval and move on to the next phase, it must prove that it has meet all technical requirements and risk assessments for the ADE as well as receive approval from the acquisition board review and organization management.[81] ADE1 is the approval for an acquisition program, categorized as a non-major acquisition, and fulfills the requirement to move from the Need phase to the Analyze/Select phase. ADE2 is the approval of the AoA, which was described in detail in Chapter II, identified through market research and the approval to move into the Obtain phase. ADE3 is an authorization for the acquisition to enter the Produce/Deploy and Support phase. In Figure 3, the three ADEs are represented with triangles between each of the four main phases of the USCG Acquisition Life cycle. The implementation of these ADEs ensures the acquisition program can meet the targeted schedule and budget.

2. Deficiencies in The USCG's SDLC Process

In 2018, GAO examined the IHiS project to evaluate whether the USCG applied the principles of the SDLC process and if the IHiS project had fulfilled the required steps in the SDLC project management practice. The review focused on: 1) conceptual planning 2) planning requirements, 3) design, 4) development and testing. The GAO report found the Coast Guard completed some but not all the elements required in the SDLC or could

[81] U.S. Coast Guard Acquisition Directorate, *Major Systems Acquisition Manual (MSAM)*, 2–3.

not provide all the documentation to show that it had completed all the elements required in the SDLC.[82]

One major flaw of the USCG's SDLC process was that it did not identify all the system's needs in the conceptual planning phase. The Coast Guard tried to meet its limited budget in the early stages and, therefore, decided to forego many costly upgrades when it first identified the system's needs.[83] However, the USCG did not stick with these limited requirements after moving to the Obtain phase.[84] Neither the USCG nor GAO indicated the reasons for adding additional requirement during the Obtain phase. However, the main cause for this late addition of requirements can be attributed to the poor AoA that the USCG executed in the previous phases. The USCG did not establish all the project's requirements in the Need phase, which negatively affected its ability to select the best service provider.

While the USCG moved to the Obtain phase for the project in 2010, it increased its requirements various times, which threatened the project's success. The USCG identified the need to upgrade the safety of data management, work-life case management, and an integrated patient portal that would allow patients to access their medical record at any time. As a result, it added a service-wide Health, Safety, and Work Life (HSWL) IT re-engineering project when it changed from EHR to IHiS in the end of 2010.[85] However, the addition of requirements in the Obtain phase increased costs and extended the schedule. In addition, in 2012, the Department of State signed an interagency agreement with the Coast Guard to employ IHiS for the State Department personnel in an attempt to keep the project costs low. Adding another user to the IHiS added even more new requirements to the system. Failure to finalize project requirements and scope effectively caused the IHiS project to suffer cost and schedule increases and jeopardized the successful implementation of the software.

---

[82] Powner, Coast Guard Health Records.

[83] Powner.

[84] Powner, 12.

[85] Powner, Coast Guard Health Records.

Without knowing the requirements in the Need phase, the USCG could not validate alignment between the project requirements with the enterprise architecture in the conceptual planning phase.[86] The validation of project requirement alignment would have identified that IHiS did not meet the USCG Health Care program's objectives at an early stage. Neither the USCG nor the GAO clarified why the USCG did not validate alignment between IHiS and the USCG's health care system's operational missions. The conceptual and planning and requirement phases should have included a project description, a breakdown of work objectives with project milestones, a communication plan, project standards and procedures, and lists of personnel assigned to the selected SDLC.[87] However, the report found that the USCG did not complete or only partially completed some of the required phases in the SDLC for IHiS, possibly because of oversight issues. It also found that the work breakdown structure, project schedule, and project milestones were partially but not completely done in the planning and requirement phase. The GAO report did not explain the reasons why there were such missteps on the USCG's part; the report only indicated those deficiencies.

A further contributing factor that allowed the requirements and scope to get out of hand was insufficient ADE exit approval. The GAO reported that no documentation was provided for ADE1. ADE1 would have entailed documentation of all the necessary reviews by decision authorities to assess whether IHiS was ready to move from the Need phase to the Analyze/Select phase in the DHS Acquisition Life cycle. With completion of the ADE1 review process, the USCG and DHS management would have caught any risks or program issues. The IHiS program along with the DHS and USCG management would have had a chance to fix the issues before the IHiS program moved further along in the acquisition process.

In addition, even though the GAO 18–59 reported that IHiS received ADE2 with deficiencies,[88] because the project failed the testing in the Obtain phase, it is safe to draw

[86] Powner, 14.

[87] Powner, Coast Guard Health Records.

[88] Powner, Coast Guard Health Records.

the conclusion that IHiS did not complete all the appropriate steps to pass this ADE. The Acquisition Life cycle processes embedded in the life cycle are cumulative and connected with one another. However, without completing a solid ADE1, even if ADE2 was properly done, there would still be problems in the Obtain phase.

B. LEADERSHIP AND EXPERTISE

Four governance bodies were supposed to oversee the IHiS project: the Executive Steering Committee, the Change Control Board, the System Security Committee, and the User Group.[89] The Executive Steering Committee intended to monitor the acquisition process and approve any changes in scope and requirements for the project. The Change Control Board set out to evaluate any technical changes that would impact cost and schedule and recommend changes to the project baseline. The System Security Committee served as risk managers and helped to identify and mitigate risks for the IHiS project. The User Group served as advisors on any recommendations that would affect the functionality of the system and served as the advocate for system users.[90] The User Group committee's main purpose was to help the program office with program decisions on system design with user interests in mind.

These four committees were formed to govern and inform their recommendations to the IHiS program management office. Although these governance bodies were to oversee the IHiS project, according to the GAO report, the USCG record showed that the committees were not actively overseeing the IHiS project as they should have been before the IHiS project discontinuance in late 2015.[91] The lack of oversight from the four committees and the coordination between the committee and the program manager[92] showed weak leadership commitment for IHiS success. As mentioned in the SDLC's deficiencies section, the USCG did not fully complete the required steps in the conceptual

[89] Powner; U.S. Coast Guard, System Development Life Cycle Practice Manual, 3.

[90] The user group focuses on providing recommendations to IHiS program managers to improve IHiS functions for efficiency and effectiveness.

[91] Powner, Coast Guard Health Records.

[92] Program manager is responsible for tracking and making sure the acquisition project meet the schedule and cost target by leading a multifunctional acquisition team.

planning and planning requirements under the Need and Analyze/Select acquisition phases. Effectively completing these phases would have enabled these committees to better support the IHiS program. The lack oversight in IHiS contributed to the termination of the project.

Moreover, the CIO was not on any governance committees.[93] This could possibly be due to a lack of oversight and integration among USCG offices or it could have been negligence on the part of the USCG. The CIO should have been in one of the governance committees and should have been involved in most aspects of the system or software development and the SDLC. The CIO plays important roles in information technology acquisition. According to the Clinger-Cohen Act of 1996, CIOs are responsible for providing advice, guidance and assistance to agency heads on IT acquisition and Information Resource Management.[94] Acquisition programs related to information technology (IT) or IT connection are mandated to have the CIO sign off on each acquisition milestone. In addition, the Federal Information Technology Acquisition Reform Act requires the CIO's involvement for all federal agencies involved with the decision processes and policies related to information technology resources and all information systems and software development acquisition projects.[95] Nevertheless, in the IHiS project, the CIO was virtually absent. The facts that IHiS lacked oversight from different governance bodies and especially that the CIO was not included in one of the governance committees represented big missteps for the IHiS project. The CIO should have served as one of the stakeholders and the technical experts who would provide technical guidance and oversight to IHiS system development project to ensure the project delivery was on schedule, on budget, and could meet the program objectives.

In addition to a lack of leadership, a lack of expertise to support an acquisition program was also an issue in the IHiS acquisition. Expertise in an acquisition team usually

---

93 Powner, Coast Guard Health Records.

94 "Clinger-Cohen Act of 1996," Pub. L. No. 104–106, § Public Buildings, Property and Works, Title 40 USCODE-2011 13 (1996), https://www.govinfo.gov/content/pkg/USCODE-2011-title40/pdf/USCODE-2011-title40-subtitleIII.pdf.

95 Shaun Donovan, *Management and Oversight of Federal Information Technology*, M-15–14 (Washington, DC: Office of Management and Budget, 2015), https://www.fai.gov/sites/default/files/2015-06-10-OMB-Memo-FITARA.pdf.

includes a program manager, technical specialists, engineers, contracting officer, cost analyst, budget officer and legal advisor.[96] The composition of the acquisition team may vary and it is an interdisciplinary team who work together to meet the requirements and the objectives of an acquisition project. Change in management staff and a lack of clearly defined responsibilities were listed as deficiencies in the GAO 18–59 report.[97] The GAO report cited the roles and responsibilities among stakeholders, responsible parties, and decision makers were not clearly defined because of the high staff turnover.[98] High turnover in staff could result in a shortage of expertise and therefore severely affect the project. For instance, it would normally take time for the new employees to get up to speed and familiarize themselves with the project. A study of staff turnover in acquisition, assimilation and their impact on software development projects shows that staff turnover can result in detrimental effects on programs with significant cost increases and schedule delays.[99]

Another major flaw with adequate leadership was that the USCG overlooked the legal consequences and the disruption to the acquisition process of incorporating the State Department's health care system into IHiS. Legality issues arose with collecting and using funding from the State Department.[100] GAO said that the initial reason for its review of the IHiS project was to identify if the Coast Guard misused funding without congressional approval. When a program goes through the Anti-Deficiency Act (ADA), the employees who are involved in the program could possibly be subject to penalties of fines, imprisonment, or both. The agency has to report the violation to the President and

96 *Guidebook for the Acquisition of Services: ACE for Services* (Washington, DC: Department of Defense, 2012), https://www.acq.osd.mil/dpap/ccap/cc/corhb/files/miscellaneous_training/guidebook_for_acquisition_of_services_24march2012.pdf.

97 Powner, Coast Guard Health Records, 10.

98 Powner, 9–10.

99 Tarek K. Abdel-Hamid, "A Study of Staff Turnover, Acquisition, and Assimilation and Their Impact on Software Development Cost and Schedule," *Journal of Management Information Systems* 6, no. 1 (1989): 21–40.

100 Powner, Coast Guard Health Records.

Congress.[101] Therefore, the review for the ADA alone could potentially cause a stop on the acquisition program. The GAO 18–59 report did not disclose whether the USCG had the authority to enter an interagency agreement with the State Department as a health care systems service provider.[102] GAO also did not mention anything about how the State Department requirements were incorporated into the IHiS project.[103] As mentioned in the requirements and scope section, adding the State Department to the project happened after IHiS entered the Obtain phase. Leadership clearly ignored the life cycle acquisition phases, which caused the program to increase its technical complexity in addition to possibly violating the ADA.

C. BUSINESS PROCESS CHANGE

Business process change is crucial for every acquisition project, especially the big ones. Business process change involves planning for how organizations would do their usual business using the new system. The IHiS project was in the Obtain phase for five years by the time it was terminated, so the USCG and the State Department health care work force should have been undergoing business process change during this phase. However, as the GAO report mentioned, the USCG did not develop the process changes or help the USCG or State Department health care work force get ready for the roll-out of IHiS.[104]

The user manual and the testing process were missing in the IHiS project. The manual and training would allow employees to be familiarized with the new system and help the organization smoothly transition to the new system. The user manual usually defines the policies and processes for users to follow when they use or operate a new system.[105] However, the Coast Guard did not develop a user manual that specified how to

---

101 "Antideficiency Act Resources," Government Accountability Office, accessed March 15, 2021, https://www.gao.gov/legal/appropriations-law/resources.

102 Powner, Coast Guard Health Records.

103 Powner.

104 Powner, Coast Guard Health Records.

105 "What is Process Documentation |The Easy Guide to Process Documentation," *Creately* (blog), January 29, 2018, https://creately.com/blog/diagrams/process-documentation-guide/.

use and operate the IHiS system.[106] This could be considered an internal control weakness, which was one of the deficiencies listed in the GAO report.[107]

In addition, system testing was also missing.[108] Its absence negatively impacts the buy-in process. The purpose of the testing process is to make sure the new system meets the organization's operational objectives. Users usually participate in the testing phase. Their participation enhances the buy-in process and ensures the new acquisition system meets the users' needs. In sum, the testing process validates that the new acquisition system operates properly and meets all technical and business requirements as set in the Conceptual Planning and Planning and Requirement phases in the SDLC process, or the Need and Analyze/Select phases in the DHS and USCG Acquisition Life cycle Framework.[109]

The IHiS project did not involve the users in participating in the testing of the system, did not develop a user manual, and did not include the users in the user oversight committee, all of which are main components of the business change process. Without a concrete business change process in place, the acquisition program would not be successfully implemented. In turn, the acquisition program would neither be well accepted nor add any value to the organization.

D. CONCLUSION

The GAO 18–59 reflected on the many mistakes in the IHiS project. The project lacked benchmarks for project success, so the project team could not determine whether the project was on track for completing project operational objectives. The IHiS project lacked approval or visibility to the stakeholders. Furthermore, in the Obtain phase, the USCG did not develop a training manual for use of the new health care system and added new requirements from the State Department two years after the IHiS project had begun. Moreover, the USCG did not anticipate the legality issues with collecting and using

106 Powner, Coast Guard Health Records.

107 Powner.

108 Powner, 12–13.

109 U.S. Coast Guard, System Development Life Cycle Practice Manual, 69.

funding from the State Department.[110] Consequently, in October 2015, the Coast Guard cancelled and closed out the interagency agreement with the State Department and terminated the IHiS project. Cost, schedule and technical complexity were cited as reasons for discontinuation of the project.[111] The time and money invested in the project could have been invested in an alternative product that aligned more closely with the USCG Health Care program's objectives.

Currently, the USCG has joined the DOD and the Department of Veterans Affair in using MHS GENESIS as of June 8, 2018.[112] This program is currently in the Obtain phase as the new EHR system for the Military Health System for Army, Navy, and Air Force, and the USCG. Like its predecessor, this system is an automated medical information system that supports health care administration and record keeping. The Coast Guard Health Care program is on the right track to transition from the Obtain phase to the Produce/Deploy/Support/Disposition phase.[113]

---

110 Powner, Coast Guard Health Records.

111 Heather Landi, "U.S. Coast Guard Terminated Contract with Epic for EHR Implementation," *Healthcare Innovation*, April 25, 2016, https://www.hcinnovationgroup.com/policy-value-based-care/news/13026683/us-coast-guard-terminated-contract-with-epic-for-ehr-implementation.

112 U.S. Coast Guard Acquisition Directorate, "Electronic Health Records Acquisition."

113 "MHS GENESIS," Military Health System, accessed April 9, 2021, https://www.health.mil/Military-Health-Topics/Technology/Federal-Electronic-Health-Record-Modernization/MHS-GENESIS.

IV. HEALTHCARE.GOV

This chapter reviews the HealthCare.gov project. The Centers for Medicare & Medicaid Services (CMS), operating under the Department of Health and Human Services, designed the website HealthCare.gov to facilitate health care registration under the Affordable Care Act (ACA). The ACA intended to increase health care access to all Americans. With the ACA, states can create their own health care exchanges or join the federal program via HealthCare.gov.[114] However, when it launched in October 2013 the website encountered several problems. It could not handle the number of users, it gave erroneous health care rates, and the website was down for a long period of time during the first week it was launched. In addition to failure in the first launching period, the website's development costs were expected to be $292 million but jumped to $2.1 billion, per a Bloomberg report in September 2014.[115] As a result, the GAO did a study on the HealthCare.gov project.[116] The GAO study reviewed all the systems that supported the website to address the deficiencies contributing to the website failure on the first launch, and recommended lessons learned moving forward. The report was published in March 2015.

Accordingly, this chapter identifies the factors that contributed to the project's shortcomings when it was first launched. This chapter reviews the initial efforts of the HealthCare.gov project, the deficiencies in project requirements and scope, leadership, expertise, and project business change management that led to the failures in October 2013.

---

114 "Affordable Care Act (ACA)," HealthCare.gov, accessed August 17, 2020, https://www.healthcare.gov/glossary/affordable-care-act/.

115 Alex Wayne, "Obamacare website Costs Exceed $2 Billion, Study Finds," *Bloomberg*, September 24, 2014, https://www.bloomberg.com/news/articles/2014-09-24/obamacare-website-costs-exceed-2-billion-study-finds.

116 Valerie C. Melvin, *Health Care.Gov: CMS Has Taken Steps to Address Problem, but Needs to Further Implement System Development Best Practices.*, GAO-15-238 (Washington, DC: Government Accountability Office, 2015), https://www.gao.gov/assets/670/668834.pdf.

A. BACKGROUND

The HealthCare.gov website is a public website, designed for the American public to browse health care insurance plans and enroll in a coverage plan. Some Americans who have low income are eligible for financial assistance to cover premiums and other health care insurance costs. The health care website linked to multiple support systems from other government agencies such as the Department of Health and Human Services, Internal Revenue Service (IRS), Social Security Administration, and DHS to verify individual identity and eligibility. It also linked to credit report companies like Equifax, Inc. to verify income amount. In addition, the HealthCare.gov website links to different market insurers for different health care plan options and prices. The website is, thus, one of the most complicated large-scale information technology systems in the United States government. Figure 4 is an overview of the systems supporting HealthCare.gov.

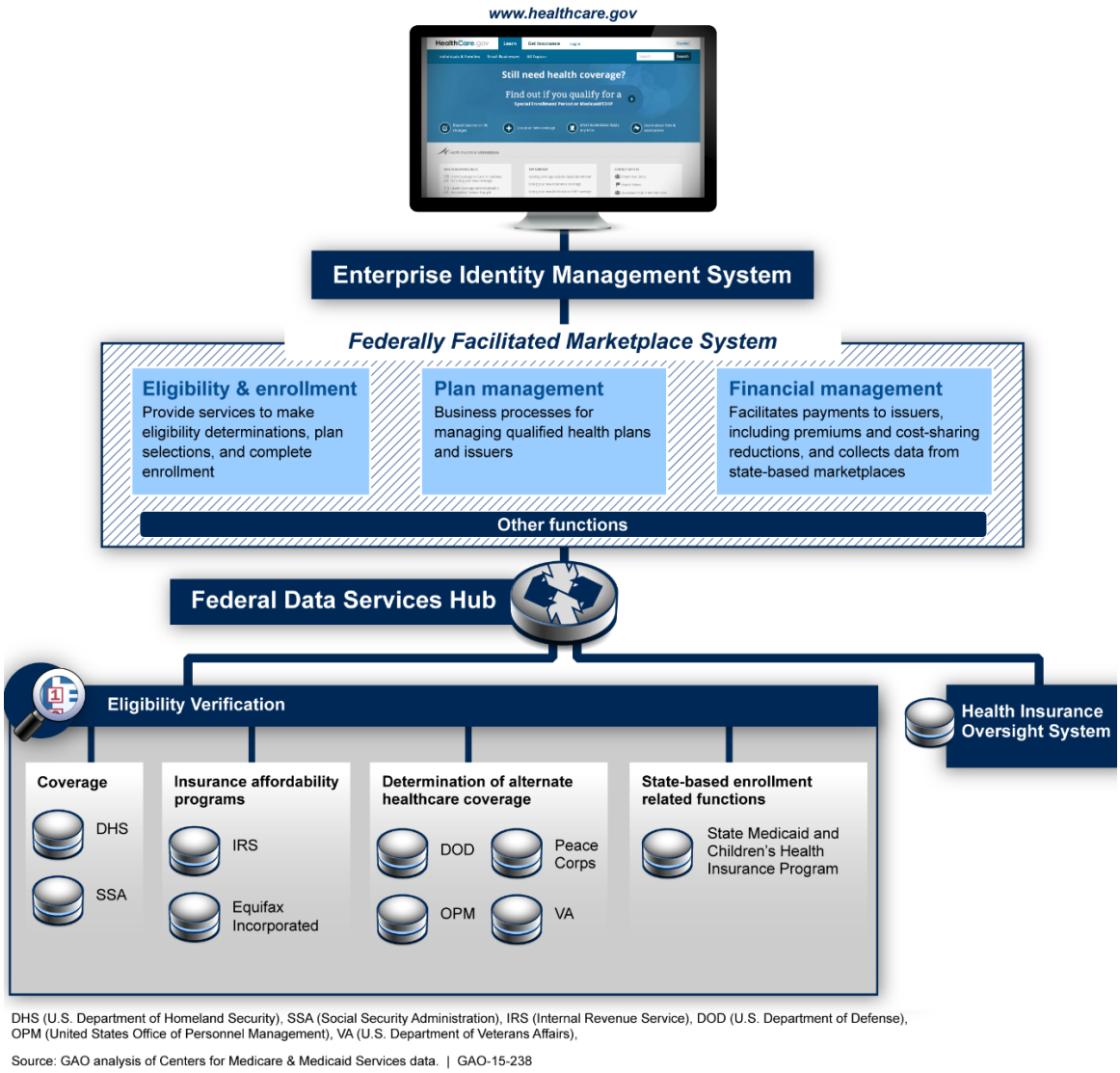

Figure 4. Overview of Systems Supporting the Federal Facilitated Market place.[117]

HealthCare.gov provides basic information on how insurance plans work through the Federal Marketplace. It includes the Enterprise Identity Management system that checks an individual's identity through his or her social security number and date of birth. The CMS Enterprise Identity Management system houses the applicants' log-in accounts and user identities. This system provides users log-in access and monitors applicants'

[117] Melvin, Health Care.Gov: CMS Has Taken Steps.

accounts at HealthCare.gov.[118] After the applicants have successfully set up their accounts through the Enterprise Identity Management system, their information transfers to the Federal Facilitated Marketplace (FFM) system.

1. Federally Facilitated Marketplace System

The GAO report describes the FFM system as a "database system that processes transactions to facilitate the eligibility verification process, enrollment process, plan management, financial management services, and other functions, such as quality control and oversight." [119] The FFM uses cloud-based services that provide data processing and storage space from private sector vendors over the Internet. The FFM consists of "three major modules: eligibility and enrollment, plan management, and financial management."[120]

a. Eligibility and Enrollment Module

The Enterprise Identity Management (EIDM) system "allows applicants to create accounts and verify their identities on HealthCare.gov and sends information requests from the Federal Marketplace (Health Insurance Marketplace) to other government agencies."[121] First, the applicants must enter their personal information such as social security number, birthdate, and address. CMS then verifies the applicant's identity though the eligibility enrollment process. The applicant's personal information is transmitted through the DHS and Social Security Administration to determine eligibility.[122] Then, individuals can apply for health care coverage through HealthCare.gov. After the applicant completes the eligibility process through the eligibility and enrollment module, he or she can begin the insurance registration process.

---

[118] Melvin, Health Care.Gov: CMS Has Taken Steps.

[119] Melvin.

[120] Melvin.

[121] Melvin.

[122] Melvin.

State, government, medical, and budget systems had to connect to the FFM system and the federal Data Service Hub (DSH). DSH supports many functions related to health care enrollment. As explained by Levinson in a report for the Department of Health and Human Services, "Most states need to connect their state Medicaid and state Children's Health Insurance Program (CHIP) agencies to either the FFM system (through the DSH) or their state-based marketplace to exchange data with CMS about enrollment in these programs."[123] In addition, several other government and non-government agencies—the Departments of Defense and VA, the Office of Personnel Management, and the Peace Corps—connect to CMS to determine if potential applicants are eligible for or currently enroll in the states and federal subsidies coverage. If they are, they would not be eligible to receive the government subsidies such as advance payment of the tax credit and insurance cost reductions.[124]

b. Plan Management Module

The plan management module is designed to facilitate the health care plans and costs among the insurance companies, health care providers, and the Department of Human Services via the CMS.[125] Health care providers and states use the plan management module to monitor health care plans. Health care providers use this module to request health care payments to the state.[126] Insurance companies also use the plan management module for bidding on or submitting the insurance plans' costs to states. CMS uses this module to review the health care plan costs, and it monitors and certifies the insurance plan bids that insurance companies and states submit.[127] Once the insurance company passes the bidding process and receives approval to participate in the health care market place

[123] Daniel R. Levinson, *HealthCare.Gov: CMS Management of the Federal Marketplace: A Case Study*, OEI-06-14-00350 (Washington, DC: Department of Health and Human Services, 2016), https://oig.hhs.gov/oei/reports/oei-06-14-00350.pdf.

[124] Melvin, Health Care.Gov: CMS Has Taken Steps, 8.

[125] Melvin, Health Care.Gov: CMS Has Taken Steps.

[126] Melvin.

[127] Melvin.

through HealthCare.gov, the insurance companies offer health care plans available for the applicant to select and enroll.[128]

c. Financial Management Module

Participating insurance companies submit and receive health care payments through the financial management module.[129] Although not all 50 states participate in the ACA, all participating states, along with CMS, use this module to calculate payments and cost reductions through subsidies polices, and to set the price for applicants' health care insurance plan. This model is used to calculate insurance plan cost and process payment between CMS and insurance companies.

2. The Federal Data Service Hub (DSH)

The Federal DHS processes and transfers information related to health care and cost among FFM, CMS, private sectors, other government agencies, and states. States relay the health care plan and applicant's personal information to the IRS through the Federal DSH; in return, the IRS gives states the subsidy eligibility amounts, such as advanced payments of premium tax credits. The DHS is a "cloud service" that processes all the information related to eligibility, enrollment, and plans.[130]

3. CMS Health Insurance Oversight System

Once the applicants have completed the enrollment process, the CMS Health Insurance Oversight System would issue the health care plan via the FFM system. The health care plans would be available via HealthCare.gov. The CMS Health Insurance Oversight System processes applications and sends out health care insurance plan through FFM. CMS monitors and controls the Health Insurance Oversight System.

---

[128] Levinson, HealthCare.Gov: CMS Management.

[129] Melvin, Health Care.Gov: CMS Has Taken Steps.

[130] Melvin, 8.

B. PROJECT REQUIREMENTS AND SCOPE

As soon as HealthCare.gov was launched and opened to the public on October 1, 2013, the website encountered many problems. A lot of issues derived from not defining the requirements in a timely manner. Defining scope and project requirements should have happened in the first phase of the acquisition, the Need phase. However, the political effects of the ACA law had negative effects on the project requirements.[131] For instance, CMS and HHS wanted states to have autonomy to either create and maintain their own insurance marketplaces or to join the Federal Marketplace.[132] Some states were against the Federal Marketplace, and in these cases the CMS would revise policy to give more flexibility to accommodate these states.[133] The Department of HHS Office of Inspector General's (HHS OIG) report indicated that "CMS's lack of clarity in defining key marketplace functions, which traces back to conflicting statutory interpretation and debates about policy choices," resulted in CMS's inability to lock down the requirements and scope.[134] All these changes triggered late changes in the scope and project requirements that would in turn delay the project and cause technical issues later since the requirements were not properly vested and were not finalized before the project moved to the next phase of the acquisition process.

Another issue with HealthCare.gov was that the program did not lock down the requirements early in the acquisition process as it should have done. All the system requirements should have been firmly established in the Initiation and Planning Phase and Requirement Analysis and Design Phases (see Figure 5), which are similar to the DHS Need phase and Analyze/Select Phase. Instead, the HHS employees were under schedule pressures to launch the HealthCare.gov website on time regardless of the issues during the development phase.[135] Moreover, the HealthCare.gov project stagnated because the ACA law was under Supreme Court review for almost two years to determine whether the law

131 Levinson, HealthCare.Gov: CMS Management, 11.

132 Levinson, 11.

133 Levinson, 31.

134 Levinson, HealthCare.Gov: CMS Management.

135 Levinson.

could mandate individuals to purchase health insurance.[136] These challenges to the law caused uncertainties regarding possible changes in the implementation of the ACA and, therefore, the HealthCare.gov website. As of June 2012, the Supreme Court ruled that the ACA, including the mandate for individual Americans to buy health insurance, was constitutional.[137] However, the final decision from the Supreme Court was only just over a year before the HealthCare.gov website was to be launched in October 2013 and all the final changes in the requirements were supposed to have already been built into the website. CMS continued to make changes in policy along with technical and business requirements up to early 2013, just a few months before the website launch on October 1, 2013.[138] Ultimately, the last-minute changes caused the CMS and contractors who developed the HealthCare.gov website to run out of the time needed to test and fix the errors before the launch. The last-minute changes caused the HealthCare.gov website not to provide the correct insurance plan rates based on the applicants' information submitted and processed through three modules, "eligibility and enrollment, plan management, and financial management."[139] Figure 5 shows the Enterprise Life Cycle Model, a guideline for information system from CMS which includes progress reviews and three major acquisition phases: Initiation and Planning, Development and Implementation, and Operations and Maintenance.

---

136 Levinson.

137 Thompson, K., "Supreme Court Ruling on the Affordable Care Act," *NAFC, The National Association of Free & Charitable Clinics* (blog), November 10, 2020, https://www.nafcclinics.org/content/supreme-court-ruling-affordable-care-act.

138 Levinson, HealthCare.Gov: CMS Management.

139 Melvin, Health Care.Gov: CMS Has Taken Steps.

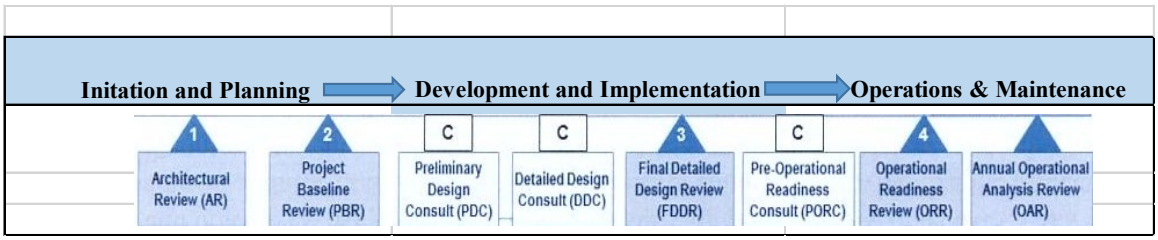

Figure 5. IT Enterprise Life Cycle Model.[140]

All the late changes and attention to policy instead of careful website development caused delays in the schedule. The ACA was one of the most contentious laws in U.S. history. As of 2017, there had been more than 70 attempts to repeal it since it was first signed into law on March 23, 2010.[141] The deadline for states to set up and manage their own insurance marketplaces or to participate in the Federal Marketplace supported under the law was extended to December 2012.[142] The number of states joining the Federal Marketplace affected health care coverage and also affected policy and content of the website.[143] Many policy changes that required software changes to support the HealthCare.gov website arose late in the development phase. CMS continued to make changes in policy along with technical and business requirements up to early 2013, just a few months before the website launched on October 1, 2013.[144] While the delayed changes in the requirements were outside of CMS's control, these late changes hindered the project's success.

CMS underestimated the number of potential applicants who would visit the website, which negatively impacted the site's performance. The HealthCare.gov site experienced many operational issues as soon it was open for public use. The website crashed within two hours after being launched and only six applicants completed their

[140] Centers for Medicare & Medicaid Services, *Guide to Enterprise Life Cycle Processes, Artifacts, and Reviews*, Version 1.1 (Washington, DC: Department of Health and Human Services, 2012), 27, https://medicaid.ms.gov/wp-content/uploads/2014/03/Appendix-K-CMS-Enterprise-Life-Cycle.pdf.

[141] Chris Riotta, "GOP Aims to Kill Obamacare Yet Again after Failing 70 Times," *Newsweek*, July 29, 2017, https://www.newsweek.com/gop-health-care-bill-repeal-and-replace-70-failed-attempts-643832.

[142] Levinson, HealthCare.Gov: CMS Management.

[143] Levinson.

[144] Levinson.

enrollment on that first day.[145] The HealthCare.gov website was opened for public use with inadequate capacity to handle the number of applicants. According to HHS OIG's report in February 2016, approximately 250,000 users logged into the website on its first day, which far exceeded its built-in capacity.[146] The surge caused the website to run very slowly and sometimes took it offline completely.[147] Applicants received error messages and some who successfully created accounts had difficulty in logging in.[148] The website was not built with enough capacity for an adequate number of virtual machines and processes.[149] According to the HHS OIG's report, the HealthCare.gov website was down more than 50 percent of the time in early November 2013.[150] By the end of November 2013, the website availability improved to 90 percent. However, according to HHS Office of Inspector General, the "website outage during the first month of its launch" caused a lot of confusion and frustration for the users who tried to enroll in a health care plan or find out the available health care plan options.[151] There were two enrollment periods: October 1, 2013 to March 31, 2014 and from November 15, 2014 to February 2015. CMS reported that there were over eight million individuals who applied and selected their health care plans during the first enrollment period. During the second period of enrollment, over an additional 8.8 million Americans had submitted their applications as of January 2015.[152] In the congressional testimony in November 2013, the CMS administrator admitted that the agencies had underestimated system demand and failed to appreciate the complexity of HealthCare.gov.[153]

---

[145] Levinson.

[146] Levinson.

[147] Melvin, Health Care.Gov: CMS Has Taken Steps.

[148] Melvin, Health Care.Gov: CMS Has Taken Steps.

[149] Melvin.

[150] Levinson, HealthCare.Gov: CMS Management.

[151] Levinson.

[152] Levinson.

[153] Melvin, Health Care.Gov: CMS Has Taken Steps.

The lack of clearly establishing the site requirements and testing the site's functions before the site was launched created technical difficulties rendering the site unable to perform its main functions. In February 2014, the Federal Market system that linked to the three modules that interconnect within the HealthCare.gov site—eligibility and enrollment, plan management, and financial management—did not process 2.6 million applicants' information correctly.[154] For example, the Office of Inspector General found that "the Federal Marketplace was not able to validate an applicant's social security number."[155] This problem should have been identified in the Initiation and Planning phase. After the review, HHS OIG concluded that there were some issues with FFM internal control measures. For example, FFM failed to verify applicants' social security numbers in the beginning of the process as it was designed to.[156] If these systems measures properly worked as checkpoints, the HealthCare.gov website would have been able to provide proper rates for applicants. Since the requirements had not been clearly defined and vetted by the system stakeholders, including the project owner and developer, the project failed to meet the requirements and operational objectives. In this case, CMS failed to estimate the required capacity for the website and clearly failed to understand how the website would operate to meet the ACA's objectives. In sum, CMS failed to understand the scope and to lock down the requirements in accordance with the Acquisition Life cycle process, which negatively affected the project.

C. LEADERSHIP AND EXPERTISE

Having the right expertise and strong leadership plays an important role in the success of big acquisition projects such as HealthCare.gov. However, there were many issues in leadership and expertise for the HealthCareg.gov project such as high turnover in leadership positions, a lack of information system and engineering skills, and leadership's failure to utilize the management tool to provide oversight to the program.

---

154 Levinson, HealthCare.Gov: CMS Management, 48.

155 Levinson, 48.

156 Levinson, HealthCare.Gov: CMS Management.

One of the most crucial assets for any project is human capital. With the HealthCare.gov project, many employees in HHS involved in the development of HealthCare.gov had experience in the insurance market but did not have any experience with information technology, system development, or managing the development of a large and complex government project such as the HealthCare.gov.[157] This lack of expertise would have serious consequences for the project such as poor technical decisions, not being able to translate policies to technical needs, not being able to help the program meet the policy requirements, and the site's poor performance and usability. One example that OIG pointed out was "CMS continued on a failing path to developing HealthCare.gov despite signs of trouble, making rushed corrections shortly before the launch that proved insufficient and CMS made poor connections between policy and technical work."[158] The lack of expertise in engineering and procurement led to bad acquisition decisions.

The project's high turnover rate of key leadership positions stretched other employees too thin and allowed for many details to be overlooked. According to the HHS OIG review, the HealthCare.gov project had a high turnover rate in many key and staff positions, which created vacancies that increased the workload and stress and reduced the organizational knowledge and relationships among staff.[159] CMS had a high turnover especially among the staff who supported the Federal Marketplace program as CMS lost many management positions who were under the CIO Office.[160] Personnel in the CIO Director- and Deputy-level positions often held these roles for less than one year from 2011 to 2015.[161] One management position in the program—a director position—was filled by seven different incumbents in the four year period from 2011 to 2015. HHS OIG conducted their review of the HealthCare.gov program's operation from 2011 to 2015, and found that the high turnover was mostly due to heavy workload and short deadlines.[162] The HHS OIG

[157] Melvin, Health Care.Gov: CMS Has Taken Steps.

[158] Levinson, HealthCare.Gov: CMS Management, 4;20.

[159] Levinson, HealthCare.Gov: CMS Management.

[160] Levinson, 20.

[161] Levinson, 3.

[162] Levinson, HealthCare.Gov: CMS Management.

also discovered 30 of 45 the Director- and Deputy-level positions were unfilled during those four years. In addition, in that period of time, CMS filled those vacant positions with staff who were temporarily assigned from other parts of CMS to serve in an "acting" or temporary capacity, according to HHS OIG.[163] The acting capacity can have negative consequences for the project: those employees would serve multiple positions and divide their attention between their acting and their regular assigned positions. The acting roles affected the leadership in CMS because employees could not provide all the needed attention to the project. In addition, the OIG report also pointed out that one of the important positions that was responsible for managing "premium rates" at CMS was vacant for about two years from 2011–2013.[164] There was significant turnover in many CMS staff positions that managed and oversaw the Federal Marketplace contracts.[165] In sum, the high turnover rate and the long-term vacancies made it difficult to pass down the organizational knowledge and technical skills and made it harder for the CMS to collaborate.

Since the HealthCare.gov website must interface with different government and private sectors including insurance companies' information systems, CMS had greatly underestimated the complexity that required great leadership and oversight. The failure in leadership is reflected through their deficiency in reviewing and approving the program milestones and progress reviews. For instance, as described in the GAO report, CMS designated the FFM, DSH, and EIDM systems to be highly complex systems. CMS guidance recommends an IT project to go through the IT Enterprise Life Cycle reviews as listed in Figure 5 and in Table 3.[166] In spite of this, "the three systems did not undergo all the recommended reviews in the IT Enterprise Life Cycle."[167] Table 3 describes the review sequence in the IT Enterprise Life Cycle process.

[163] Levinson.

[164] Levinson, HealthCare.Gov: CMS Management.

[165] Melvin, Health Care.Gov: CMS Has Taken Steps.

[166] Melvin.

[167] Melvin.

Table 3. IT Enterprise Life Cycle[168]

Review	Purpose
Architecture	Determines whether the proposed project potentially duplicates, interferes, contradicts, or can leverage another investment that already exists.
Investment Selection	Determines if the IT project is sound and viable, among other things. The business need and objectives are reviewed to ensure the effort supports CMS's overall mission and objectives.
Project Baseline	Obtains management approval that the scope, total cost of the project and schedule that have been established for the project are adequately documented. The project management strategy is appropriate for moving the project forward in the life cycle.
Requirements	Verifies that the requirements are complete, accurate, consistent, and problem-free; evaluates the responsiveness to the business requirements.
Preliminary Design	Verifies that the preliminary design satisfies the functional and nonfunctional requirements and conforms with the CMS Technical Reference Architecture; determines the technical solution's completeness and consistency with CMS standards.
Detailed Design	Verifies that the final design satisfies the functional and nonfunctional requirements and conforms with the CMS Technical Reference Architecture; determines the technical solution's completeness and consistency with CMS standards.
Validation Readiness	Ensures that the system/application has completed thorough development testing and is ready for turnover to the formal, controlled test environment for validation testing.
Implementation Readiness	Ensures that the system/application has completed thorough integration testing and is ready for turnover to the formal, controlled test environment for production readiness.
Production Readiness	Ensures that the infrastructure contractor's operational staff has the appropriate startup and shutdown scripts, accurate application architecture documentation, application validation procedures, and valid contact information to ensure operability of infrastructure application.

168 Adapted from Centers for Medicare & Medicaid Services, Guide to Enterprise Life Cycle Processes, Artifacts, and Reviews.

Review	Purpose
Operational Readiness	Ensures that the system/application completed its implementation processes according to plan and that it is ready for turnover to the operations & maintenance team and operational release into the production environment.
Post-Implementation	Assesses how well the system/application performance meets its goals and recommends continued operations, changes to operations, or retirement.

The CMS leadership failed to utilize management tools such as progress reviews in the Acquisition Life cycle to monitor and provide oversight.[169] For example, "CMS noted that the HealthCare.gov had project process agreement for the EIDM system in January 2012 which stated that of the 11 progress and milestone reviews, with the exception of the Investment Selection Review, all ten reviews were mandated with proof for each review."[170] However, the agency could only prove that it performed four of the ten reviews despite that CMS officials claim that nine had been held (see Figure 6).[171] Consequently, the GAO reported that "CMS did not keep good records of each review, decision logs, or lessons learned for each program review."[172] These reviews are crucial to determine whether the project is on the right track for development purposes. A progress review is one of the major management tools for leadership to review the programs' progress, provide oversight, support and intervene if necessary. CMS provided evidence that they had completed some but not all the recommended reviews for DSH and FFM. Figure 6 shows the reviews a highly complex system should have had and GAO's assessment of whether those reviews were held for each system.

169 Melvin, Health Care.Gov: CMS Has Taken Steps.

170 Melvin, Health Care.Gov: CMS Has Taken Steps.

171 Melvin.

172 Melvin.

Reviews	Enterprise Identity Management system	DSH	FFM
Architecture Review	●	●	●
Investment Selection Review	n/a[1]	○	○
Project Baseline Review	○[2]	●	○
Requirements Review	○[2]	●	○
Preliminary Design Review	●	●	●
Detailed Design Review	●	●	●
Validation Readiness Review	●	●	○
Implementation Readiness Review	○[2]	○	○
Production Readiness Review	○[2]	○	●
Operational Readiness Review	●	●	●
Post-Implementation Review	○	○	○

Key:
● The review was held.
○ The review was not held.
Table Notes:
[1]The review was waived in the project process agreement.
[2]CMS officials could not demonstrate that this review was held; however, they indicated that it was performed.

Figure 6. GAO Evaluation for Progress and Milestone Reviews Held for Systems Supporting HealthCare.gov.[173]

The major system, FFM, did not have a review for the system requirements, which is another misstep for the project's leadership. According to the GAO report, most of the system requirements for the FFM were not approved by CMS officials prior to system development. GAO examined 37 FFM eligibility and enrollment functional requirements, only nine of which CMS had approved. For the remaining 28 FFM requirements, eight had been "approved after being sent to development," but CMS never approved the other 20.[174] Both the GAO and HHS OIG did not indicate how the project moved forward without going through the approval process for each functional requirement. However, these missteps in the approval process over the program's review showed the weakness in leadership. For example, CMS designated the DSH and the FFM as complex, but CMS did

[173] Melvin, Health Care.Gov: CMS Has Taken Steps.

[174] Melvin.

not go through all progress reviews as required.[175] The lack of leadership's participation and documentation in the progress reviews was the weakness in the leadership's role.

Another issue with the HealthCare.gov leadership was the use of an unfamiliar technology, which is not a recommended practice.[176] Leadership usually approves the program to follow a certain technology through the review process. For the HealthCare.gov project, CMS chose to combine two types of database platforms, one traditional and one nontraditional, instead of the commonly used traditional platform database per the HHS OIG report.[177] Oracle defines a database as an "organized collection of structured information, or data that stored electronically in a computer system."[178] The traditional platform has been around for quite some time, and it is widely used. Most engineers or IT specialists who are experienced with Oracle would be familiar with the traditional platform. However, the nontraditional NoSQL platform offers more capabilities, can transfer data faster than the traditional platform, and has the capability to add more data or users.[179] However, NoSQL platforms were not as popular and widely used as the traditional platform. There were fewer developers who had experience with the nontraditional NoSQL platform at the time of HealthCare.gov project development. Per the HHS OIG report, MarkLogic, the vendor that was responsible for the NoSQL platforms, did not have the right expertise in its team, so the use of the NoSQL platforms caused significant issues for the FFM build.[180]

Lastly, GAO reported a lack of leadership from the executive branch, the Office of Management and Budget. HHS, CMS, and the OMB were supposed to collaborate with each other to support the HealthCare.gov website development. GAO noted that the HealthCare.gov project was not included in the federal IT dashboard, monitored by

---

175 Melvin, 53.

176 Blanchette, "Pros and Cons of Using COTS Products."

177 Levinson, HealthCare.Gov: CMS Management, 24.

178 "What Is a Database?," Oracle, accessed May 10, 2021, https://www.oracle.com/in/database/what-is-database/.

179 Levinson, HealthCare.Gov: CMS Management, 16.

180 Melvin, Health Care.Gov: CMS Has Taken Steps, 25.

OMB.[181] The OMB Information Technology dashboard is used to monitor risk and performance for all federal government IT projects. Since the HealthCare.gov project was not included on this dashboard, OMB failed to perform oversight, report, and monitor risk and issues with the project costs, schedule, and performance. This lapse represents another layer of leadership failure by the OMB.

The HealthCare.gov program suffered various issues with leadership and expertise such as not having employees with the required skillsets, and was not able to fill all the key positions. In addition, the program did not have strong leadership to provide oversight and champion the program. The weakness in leadership and lack of the required skills in the HealthCare.gov program hampered the program's success.

D. BUSINESS PROCESS CHANGE

Business process change is all about communicating the changes to the stakeholders and having the stakeholders involved in the project. One of the ways to have stakeholders' involved is including them in the testing process, which helps the stakeholders become familiar with the new system and gives them an opportunity to provide their input. For the HealthCare.gov project, there were many deficiencies in the business process change, primarily in the testing process. CMS has a testing framework documented in the IT Enterprise Life Cycle guidelines that describes how to test the software before deploying it to the Operations and Maintenance Phase, yet it did not execute all the required tests for the HealthCare.gov software. For example, "in May 2011, CMS documented a testing framework that was to establish a consistent, repeatable CMS testing life-cycle process for business application and infrastructure testing."[182] In the contract document CMS required its contractors to use the testing framework to conduct testing and validate all the software releases for FMS and DHS systems prior to implementation.[183] The contract included "integration and end-to-end testing of both the FFM and DSH systems."[184] The testing

[181] Melvin, Health Care.Gov: CMS Has Taken Steps.

[182] Melvin, 33.

[183] Melvin.

[184] Melvin, Health Care.Gov: CMS Has Taken Steps.

process for different modules that allowed the FFM and other system to operate together did not happen.[185] The GAO report also indicated that if the testing for the HealthCare.gov website happened, it would have shown whether the "individual systems that support the federally facilitated marketplace work [ed] together as intended." [186] CMS and OMB would have found out that the HealthCare.gov website did not work as intended sooner and would have had opportunities to fix the website before it launched if they had followed normal a business process change.

According to the GAO report, CMS did not execute all the required testing for systems supporting HealthCare.gov as the agency was supposed to.[187] For example, just two months before the system opened for public use in August 2013, the contract team and CMS did not complete the "integration testing with plan issuers that was expected to connect to the DSH to send health plan information to the FFM plan management module."[188] In addition, the pending defects were not fixed properly for the FFM system eligibility and the enrollment module to function correctly.[189] The testing process is very important in business process change management because testing an IT system is essential to help system developers and users validate if the system meets the requirements for its intended use and satisfies the users' need. Effective testing can help identify and correct software and system errors early and that ensures assessment of system readiness in time. The testing process is used to evaluate whether the program is ready to move from the Obtain phase to the Operation and Maintenance phase. IEEE developed best practices which recommended program offices to conduct systems testing as early and as often in the life cycle of an acquisition software development project.[190] The timely and frequent testing steps allow for technical changes to occur early enough in the process, thereby

185 Melvin.

186 Melvin.

187 Melvin.

188 Melvin, 30.

189 Melvin, Health Care.Gov: CMS Has Taken Steps.

190 IEEE Computer Society, *IEEE Standard for Software and System Test Documentation*, IEEE Std 829–2008 (New York: IEEE, 2008).

reducing the chance for overall project and schedule failures. For most DHS and DOD acquisition life cycles, testing happens under the Obtain phase before moving to the transition the software to the Operation and Maintenance phase. For IT development projects under CMS, testing usually happens in the Development and Implementation phase, the third phase before the Operation and Maintenance phase in the IT Enterprise Life Cycle.[191] The GAO report further said that the "end-to-end testing of HealthCare.gov and its supporting systems did not occur prior to system launch as required. CMS did not always ensure that system defects found during the testing were corrected prior to system launch."[192] Testing is one the most crucial process in the Development and Implementation phase, and it plays a major role in business process change. Without completing the testing process, the program would not be able the detect errors, deficiencies; the system also failed to get the users and stakeholders buy-in with the new system.

As evidenced by the systems' failures when launched, many defective system components and errors were carried out into production, causing the website to fail. Two major failures were that the website could not handle the volume of the enrollment requested and often crashed, and that the technical aspects such as its assurance system were not functioning. The website could not process and produce accurate insurance rates using the identity and eligibility information. If the HealthCare.gov program went through the testing process properly, CMS would have been able to detect the problems, which would have been fixed in time. The testing process would have given all the stakeholders—in this case, the OMB, HHS and CMS leadership—opportunities to fix the website, and they may have decided to delay the launch in October 2013 until they could make sure the website ran smoothly.

E. CONCLUSION

The HealthCare.gov project has made significant improvements since its launch. The second enrollment which began on November 15, 2014 ran smoothly, and there were

[191] Centers for Medicare & Medicaid Services, *Guide to Enterprise Life Cycle Processes*, 54.

[192] Melvin, Health Care.Gov: CMS Has Taken Steps.

no outages. The HHS OIG noted that the response time when applicants clicked on the HealthCare.gov website was much faster, running at 3.1 seconds compared to 18.46 seconds during the first launch in October 2013.[193] CMS also tried to fix the technical errors with health care plans' costs and tax credits in addition to strengthening the leadership and providing more oversight on the HealthCare.gov project.[194] As of June 2015, over 9.9 million Americans completed their health care plan on the HealthCare.gov website.[195] Despite these improvements, the initial failure resulted in widespread negative publicity for the website. The initial launch failure overshadowed the objective of the ACA, which was to provide access to health care insurance for all Americans, especially those in need.

[193] Levinson, HealthCare.Gov: CMS Management.

[194] Levinson.

[195] Melvin, Health Care.Gov: CMS Has Taken Steps.

THIS PAGE INTENTIONALLY LEFT BLANK

V. FBI VIRTUAL CASE FILE

Chapter V focuses on the fourth case study, the FBI VCF. It provides the lessons learned, and describes the challenges faced by the VCF project. The FBI's information technology system in the 2000s was antiquated and lacked data sharing capability. By the early 2000s, the FBI IT systems that supported the agency's practices of collecting, sharing, and accessing investigation data were very outdated and barely functioned.[196] FBI agents collected information through their work with local law enforcement, surveillance, and interviews.[197] They then would process paperwork by filling out a paper form, faxing or sending the investigation data via FedEx up their chain of command, either to the supervisor or special agent in charge to accept the information and log it into an FBI system to officially document the data.[198] The FBI could not effectively preserve or share the investigation information among field offices or internally with FBI agents.[199] Essentially, the FBI could not efficiently access information related to terrorism, criminal cases, or share investigation information agency wide. The FBI's inadequate IT system attracted headlines in the news. Under these circumstances, the VCF project was designed to help the FBI achieve greater data sharing and better support for FBI investigative missions.

In September 2000, the FBI received $379.8 million for a three-year project to upgrade the FBI's technology system.[200] The upgrade of the IT efforts—named Trilogy—included three parts. The first part upgraded FBI computers, desktops, scanners, printers and servers. The second part upgraded and secured local-area and wide-area networks. The first two parts, upgrading hardware and networks, were to support the automated case

196 Goldstein, "Who Killed the Virtual Case File?," 4.

197 Department of Justice, Office of the Inspector General, *Federal Bureau of Investigation's Management of Information Technology Investments*, Audit Report 03–09 (Washington, DC: Department of Justice, Office of the Inspector General, 2002), 20, https://oig.justice.gov/reports/FBI/a0309/final.pdf.

198 Goldstein, "Who Killed the Virtual Case File?," 7.

199 Goldstein, 5.

200 Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project*, Audit Report 05–07 (Washington, DC: Department of Justice, 2005), 17, https://oig.justice.gov/reports/FBI/a0507/final.pdf.

support system (ACS) to run more efficiently. The VCF was the last effort in the Trilogy project and is the focus of this chapter. The VCF was designed to retain investigation data as virtual case files to replace the old, paper-based system with the ACS.[201] The ACS system[202] was one of the top five applications used within the FBI. The other four were IntelPlus, the Criminal Law Enforcement Application, the Integrated Intelligence Information Application, and the Telephone application, all accessible via Internet.[203] These five investigation applications were also referred to as User Applications Components (UAC).[204] While they were all accessible online, the main problem with the system was that each of the five applications were not connected to each other. The VCF system was meant to integrate them all into one web-based system.

The VCF was intended to help FBI agents share data to process active investigation cases more efficiently. The VCF system was designed by Science Applications International Corp (SAIC) under the FBI's oversight. The contract was awarded to SAIC in June 2001 and the VCF originally was supposed to be completed by mid-2004.[205] Then, September 11 occurred causing Congress to realize the urgency to upgrade the FBI information sharing system. The FBI received additional funding to upgrade the VCF project.[206] However, four years into the project, after spending over $170 million, a lack of clear requirements and scope for the project, a lack of leadership and expertise, as well as insufficient business process change led to the cancellation of the VCF project with

---

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

202 Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management of the Trilogy Information*, 16. From the report: "At the outset of the Trilogy project, the UAC was intended to replace each of the following five primary user applications: ACS, the FBI's primary investigative application; IntelPlus, which allows scanning, importing of electronic documents, and full-text retrieval capabilities; the Criminal Law Enforcement Application (CLEA), a repository of criminal investigation data; the Integrated Intelligence Information Application (IIIA), which supports counterintelligence and counterterrorism investigations by enabling the collection, collation, analysis, and dissemination of intelligence; and the Telephone Application (TA), which provides a central repository for telephone data obtained from investigations."

203 Department of Justice, Office of the Inspector General, The Federal Bureau of Investigation's Management of the Trilogy Information, 30.

204 Department of Justice, Office of the Inspector General, 4.

205 Department of Justice, Office of the Inspector General, 5,6.

206 Department of Justice, Office of the Inspector General, 20–22.

SAIC in April 2005.[207] Subsequently, the FBI continued its efforts to obtain an automatic electronic investigation system with different vendors and changed the project name to "Sentinel" in May 2005.

This chapter reviews how the VCF project defined project requirements and exercised leadership, expertise, and business process change throughout the Acquisition Life cycle. Finally, the case study ends with what went wrong with the VCF and what has become of Sentinel after the VCF project was terminated.

A. PROJECT REQUIREMENTS AND SCOPE

The FBI made many missteps in establishing project requirements and scope. First, it lacked an enterprise architecture that described how VCF would support the FBI operational mission. As a result, the project started with vague project needs that did not capture all the system needs. However, later in the Acquisition Life cycle, more detailed project requirements emerged. All these issues in project requirements and scope increased the complexity of the project and resulted in an unsuccessful project.

1. Underestimated Requirements

FBI system control and information access should have been key requirements for the VCF project. One of the FBI's needs from the VCF system was to balance between system control to meet security and legal requirements against having information accessible for its operations. The FBI agency collects a vast amount of information, and FBI agents need to access that data for their investigations and other operational missions. However, privacy laws such as Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act commonly restrict access to that information, which can be extremely important for FBI agents. Therefore, the information that FBI agents enter into the agency system must be secure but still accessible for the agents. If the VCF system makes information inaccessible to agents then agents may not enter or share important information at all. Instead, "agents or other information collectors may be inclined to keep two sets of records—one for official use and one for

[207] Goldstein, "Who Killed the Virtual Case File?," 5.

more sensitive information—allowing them to maintain control over the disposition of sensitive information." [208] This way, FBI agents would ensure they could still access such data in a timely way. However, their old paper-based system used hundreds of forms and required more than 20,000 access controls to conduct the agency's business[209] The VCF system needed to simplify the amount of forms used and needed to keep data secure but still accessible to certified personnel. One of the main struggles in the development of the VCF system was to ensure it met these operational, security, and accessibility goals at the same time. Identifying these specific needs at the beginning of the project was necessary to be able to design an IT system that met the security requirements and gave FBI agents both needed access and system control. However, the process of identifying VCF security and operational requirements did not happen.

The project experienced an increase in scope about six months after the project started in June. The FBI signed the contract to begin upgrading the Trilogy project in mid-2001; then the September 11 attack and the Hanssen espionage happened.[210] These two events exposed the weaknesses of the FBI electronic case file system, so the FBI added additional requirements to the VCF part of the Trilogy project. According to the OIG report on the Trilogy IT modernization project, after September 2011 the project scope increased by 80 percent.[211] The additional requirements included shortening the project duration to less than three years. After the September 11 events, the FBI mission included "terrorist investigations" in addition to criminal investigations. Moreover, the new requirements would be to replace the entire ACS with the new VCF system instead of just upgrading the old ACS by turning the old paper file to a webpage search.[212] The additional changes, both

---

[208] James C. McGroddy and Herbert S. Lin, eds., *A Review of the FBI's Trilogy Information Technology Modernization Program* (Washington, DC: National Academies Press, 2004), https://doi.org/10.17226/10991.

[209] Goldstein, "Who Killed the Virtual Case File?"; Israel, "Why the FBI Can't Build a Case Management System."

[210] Department of Justice, Office of the Inspector General, The Federal Bureau of Investigation's Management of the Trilogy Information, 18,37.

[211] Department of Justice, Office of the Inspector General, 37.

[212] Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management of the Trilogy Information,* 19; Goldstein, "Who Killed the Virtual Case File?," 6.

in scope and schedule, complicated the VCF project, which already lacked well-defined requirements.

The FBI did not have clear and locked requirements in the first stage of the acquisition process, the Need phase, in mid- and late 2000 when the agency began the project.[213] According to the 2005 congressional testimony of FBI director Robert Mueller, the FBI had not come up with completed requirements for the VCF when the agency entered the Obtain phase in June 2001.[214] The FBI had a general idea that it needed to upgrade its electronic case management system, which supported the agency with its investigation mission, but it failed to define the specific requirements needed. The original requirements the FBI defined were to upgrade the UAC from the outdated 1980s technology to an easy click-and-search capability so FBI agents could access investigation information more efficiently in the FBI investigation database.[215] However, the requirements did not include the details of how the upgrading would work with the FBI's current and future software and hardware. This vague requirement was documented in the Department of Justice OIG report. The report explained that the VCF project requirement were not based on thorough planning that included the agency's operational needs but rather was what some FBI IT managers' assumed would be beneficial for the agents to do their daily jobs.[216] As a result, the VCF project had deficiencies later in the Acquisition Life cycle. Long after the VCF program started, and as of 2004, the FBI could not make "comprehensive and consistent operational or technical decisions on how to link the FBI database of investigative information."[217] The FBI did not have the data sharing policies

213 Department of Justice, Office of the Inspector General, The Federal Bureau of Investigation's Management of the Trilogy Information, 18.

214 Robert S. Mueller, III, "Testimony • FBI's Virtual Case File System," Federal Bureau of Investigation web archive, accessed August 29, 2021, https://archives.fbi.gov/archives/news/testimony/fbis-virtual-case-file-system.

215 Department of Justice, Office of the Inspector General, The Federal Bureau of Investigation's Management of the Trilogy Information, 19.

216 Department of Justice, Office of the Inspector General, 30.

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

and methods that would guide the agency to make trade-off decisions between security and information access in the creation of their investigation information system.[218]

The FBI failed to understand the complexity of the project, which stemmed from not fully defining the project requirements, and this put the VCF project at risk of failing to meet the cost and delivery schedule. Before Congress in 2005, FBI director Robert Mueller also confirmed that the agency did not capture all the complexity of the system migration, integration, or document all the security and operational needs in VCF. The underestimation of the project requirements further showed the fact that the FBI did not fully capture all IT inventory that needed to be migrated and integrated from the old system to the VCF. The underestimation of the inventory system caused delays in schedule. For example, the IT project manager said that the FBI failed to estimate how network traffic would be slowed "once all 22,000 users came online."[219] Subsequently, when the VCF began testing the system in December 2003, there were many system failures, and the FBI decided to reject the delivery.

2. Enterprise Architecture

The agency's needs should have been captured and well defined in the initial project requirements. Figure 7 depicts the FBI organization, business activities, and strategic goals. This information should have been used to help develop the enterprise architecture document.

[218] McGroddy and Lin, A Review of the FBI's Trilogy Information.

[219] Goldstein, "Who Killed the Virtual Case File?," 10.

Figure 7. FBI Organization and Activities.[220]

The FBI entered the first acquisition phase for the Trilogy project without an enterprise architecture.[221] An enterprise architecture is similar to a CONOPS, as the process to come up with the enterprise architecture occurs in the first phase of the Acquisition Life cycle, the Need phase. A new project should begin with a business case study that documents the agency's current operational needs, compares the current system available versus the agency's needed system, and evaluates how the new system would help the agency. In sum, an enterprise architecture is a process that maps the organization, the current state of its IT infrastructure, and the IT infrastructure's future state with well-

[220] Adapted from McGroddy and Lin, A Review of the FBI's Trilogy Information, 19.

[221] Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management of the Trilogy Information*, 10. Enterprise architecture is a process that maps the organization, IT infrastructure as of current state and the future state with organization's well-defined goals and objectives.

defined project goals and objectives.[222] For the VCF, the FBI should have had a process map that described how the VCF would help FBI operational missions such as criminal identification, criminal investigation, criminal apprehension and prosecution support. The process map would have also described the migration process from the FBI's current system, ACS, to the VCF system and how the VCF would add value to Intelligence and Counterintelligence missions. Finally, the enterprise architecture also should have planned how the VCF connected to the FBI's other infrastructure such as Research and Laboratory and how VCF would contribute to the law enforcement training programs. Figure 8 shows the process map that National Academies attempted to design to help the FBI start the enterprise architecture process.

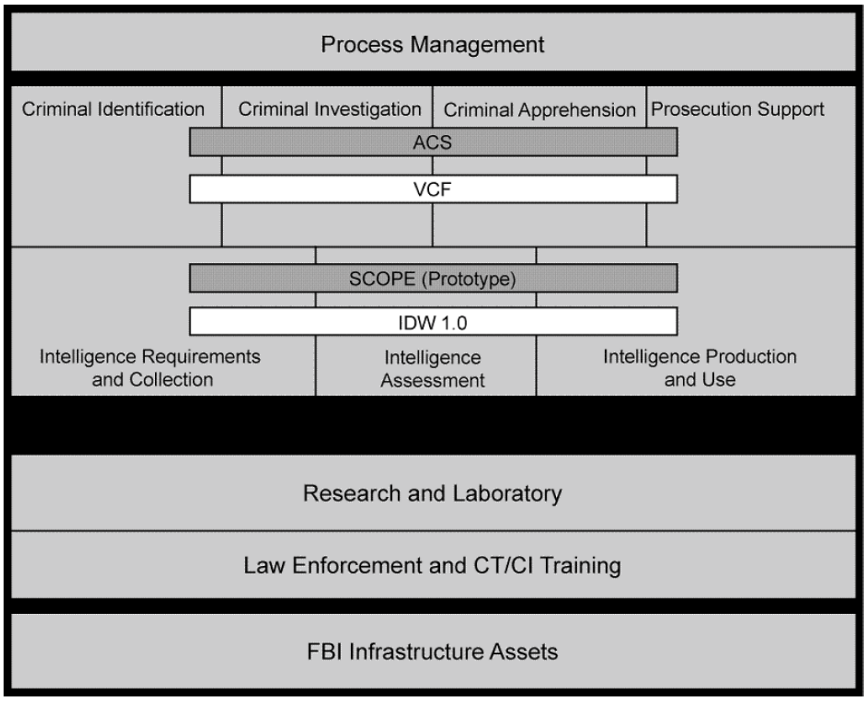

Figure 8. FBI Process Map for VCF.[223]

[222] Department of Justice, Office of the Inspector General, The Federal Bureau of Investigation's Management of the Trilogy Information.

[223] McGroddy and Lin, A Review of the FBI's Trilogy Information, 20.

Without an enterprise architecture, the FBI could not come up with a meaningful measure of progress on the project. The GAO issued a report that specifically called for the FBI to come up with an enterprise architecture for the project and the National Academies had issued warnings to the FBI on the risks of continuing the Trilogy project without an enterprise architecture.[224] Both reports also found that the FBI needed—and should actually have had—an enterprise architecture in place for the VCF to be implemented successfully. However, in 2002, over a year after VCF was in development, the FBI still did not have an "enterprise architecture and did not have all the written policies and processes in place to develop one."[225] The FBI began the VCF project in 2000 but Mueller testified that it did not begin to develop the enterprise architecture until 2004.[226] After the FBI ended the contract with SAIC in 2005, the FBI had to remap the IT process backward by using the agency's current technology and future needs to come up with a gap analysis and an enterprise architecture document. The Trilogy project resulted in many technical issues that ultimately caused cost increases and schedule delays.

If VCF had an enterprise architecture document, the agency would have had a clear process map. The enterprise architecture would explain how the VCF supported FBI missions and met operational, security, and user objectives. However, the FBI did not establish clear requirements for the VCF project and failed to complete the enterprise architecture in the Need phase. As a result, the VCF requirements kept changing as the project progressed. The acquisition process is a progressive process and the agency did not lock down or reset when project changes occurred, which had detrimental effects on cost and schedule because no project cost and schedule baseline existed for the contractors and project team to follow. Therefore, there was no preventive, performance measurement to use. The result was that the FBI management could not make sound decisions regarding balance between technical and operational requirements. Without the enterprise

---

224 Randolph C. Hite, *Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*, GAO-03-959 (Washington, DC: General Accounting Office, 2003), https://www.gao.gov/assets/gao-03-959.pdf; McGroddy and Lin, *A Review of the FBI's Trilogy Information*.

225 Hite, Information Technology: FBI.

226 Mueller, "Testimony • FBI's Virtual Case File System."

architecture, the FBI essentially failed to capture what and how the VCF would help agents to perform day-to-day operations.

B. LEADERSHIP AND EXPERTISE

Strong leadership and the right expertise play a crucial role in IT projects' success. Like previous case studies, the VCF project suffered greatly from the high turnover in many positions that supported the project: the VCF went through 15 different key IT managers and five chief of information officers, or acting chief of information officers from 2000 – 2005.[227] With high turnover in key positions, the program lost its continuity and program experience, which resulted in a lack of effective program management.

In addition to the high turnover rate, the leadership's support for the project was also weak. For example, according to the Justice Department OIG report, the IT project managers did not follow policies and procedures for IT project management, and FBI did not follow an IT investment framework.[228] Table 4 presents five critical processes of the Basic IT Investment Management Framework that the FBI should have implemented by 2002, but for reasons unspecified in the OIG report, the FBI struggled to implement the five critical processes to apply the Information Technology Investment Management (ITIM)[229] framework required by the GAO. In addition, the Department of Justice OIG reported that procedures for IT management were not well written for the FBI employees to follow.[230] This is another example of the FBI falling short of developing and implementing a complete IT investment management framework and the critical processes that go along with that framework.

---

227 Department of Justice, Office of the Inspector General, The Federal Bureau of Investigation's Management of the Trilogy Information, 41.

228 Department of Justice, Office of the Inspector General, Federal Bureau of Investigation's Management of Information Technology Investments.

229 Chuck Young, *Information Technology: Investment Management: An Overview of GAO's Assessment Framework*, GAO/AIMD-00-155 (Washington, DC: General Accounting Office, 2000), https://www.gao.gov/products/aimd-00-155.

230 Department of Justice, Office of the Inspector General, The Federal Bureau of Investigation's Management of the Trilogy Information, 27.

Table 4. Five Critical Processes of the Basic IT Investment Management Framework[231]

Critical Processes	**FBI Status of Implementing Critical Process**
Defining investment review board operations	Not implemented
Developing a basic process for selecting new IT proposals	Partially implemented
Developing project-level investment control processes	Not implemented
Identifying IT projects and systems	Not implemented
Identifying the business needs for each IT project	Not implemented

The lack of strong leadership in the VCF project was the result of the FBI not fully following the ITIM framework,[232] resulting in bad decisions being made for the project. For example, not following the framework affected the type of contract taken. Since the FBI did not fully understand the project requirements, the agency leadership decided to use the cost-plus-award-fee type of contract. This type of contract is usually used in research with unknown requirements or preliminary exploration per Federal Acquisition Regulation (FAR) Law, part 16.306.[233] A cost-plus-award-fee contract was bad for Trilogy for various reasons. First, in a cost-plus-award-fee contract, contractors are not required to complete specific milestones, which are critical decision review points. Consequently, there were no penalties or incentives for the contractor to meet the cost and schedule requirements. Second, the contractor that supported Trilogy, SAIC, was only required put in their best

231 Adapted from Department of Justice, Office of the Inspector General, Federal Bureau of Investigation's Management of Information Technology Investments, 40.

232 Department of Justice, Office of the Inspector General, Federal Bureau of Investigation's Management of Information Technology Investments, 3.

233 "Cost-Plus-Fixed-Fee Contracts," Code of Federal Acquisition Regulations, Electronic Code of Federal Regulation (e-CFR), Title 48 (2014 comp.): 16.306 §, accessed September 10, 2020, https://www.govinfo.gov/content/pkg/CFR-2019-title48-vol1/pdf/CFR-2019-title48-vol1-part16.pdf.

effort for the project.[234] Third, if the FBI would not reimburse the cost, the contractor could stop work with no penalties. Consequently, the cost-plus-award-fee procurement vehicle was a much riskier contract choice compared to other contract vehicles.

Weak leadership resulted in the project missing progress reviews, which put the project at an even higher risk for failure. Progress reviews are one of the management tools that helps management to keep the project on the right course and allow for intervention before it is too late. Since the VCF project started in 2000, the FBI did not have an acquisition framework with milestones or progress reviews before the point when FBI received the first delivery from SAIC in December 2003, which was when the FBI began to see issues with VCF.[235] The lack of strong leadership through developing and following the IT management framework, high turnover in many key positions and lack of expertise in software engineering and procurement were other contributing factors of the VCF failure.

C. BUSINESS PROCESS CHANGE

FBI modernization efforts involved in organizational and technological changes required an agency-wide buy-in process. Not enough users had vetted prototypes to win this degree of acceptance. User testing and vetting processes would have increased the likelihood of system success. Having real users testing the system would have helped IT contractors catch system errors and receive timely feedback; involvement from users would have greatly benefitted the project.

The FBI was involved in bringing the VCF online, but the agency did not vet the process that would be required to train thousands of its employees, agents, and analysts to use the VCF system. Furthermore, if the agency had had an enterprise architecture, it would have helped the FBI to articulate all the agency's needs for the VCF. The enterprise architecture would have helped the agency through the process map and gap analysis to

[234] Department of Justice, Office of the Inspector General, The Federal Bureau of Investigation's Management of the Trilogy Information.

[235] Goldstein, "Who Killed the Virtual Case File?," 11.

balance between the technical and security issues, such as how to meet the FBI's usage of form and control access and migrating data from ACS to VCF.

The FBI should have implemented a key component of business process change from the beginning of the project: user input. Users of the system should have been consulted when defining the system's requirements instead of relying only on IT managers' attempts to define the needs. An enterprise architecture and strong business process change would bring FBI employees and all stakeholders together for the modernization effort of transitioning from ACS to VCF.

In addition to the lack of user involvement, it appeared that there was not enough coordination among different stakeholders in the VCF project, such as coordination among the IT, finance, and contracting divisions supporting the Trilogy projects.[236] The defined requirements were disconnected from the actual user needs. The contract choice was not a well-thought-out process. If there had been better coordination, the requirements would have been better defined which would have also allowed for a contract type that lowered the government's risk. If the project had implemented strong business process change from the beginning, the communication and collaboration needed to find a solution would have been more effective. Since the FBI did not have strong business process change, the agency failed to implement VCF.

D. CONCLUSION

The VCF project provides many lessons learned. In short, the FBI's weak project management, failure to define the Trilogy project requirements, weak leadership, lack of expertise, and weak business process change contributed to cost and schedule overruns and the FBI spent over $170 million without results. The VCF project with SAIC was cancelled. The FBI director at the time, Robert Mueller, faced multiple congressional hearings about VCF. The project spent hundreds of millions of dollars and endured much scrutiny from Congress for these cost and schedule overruns. The initial failure of VCF can be traced back to the problems from the beginning of the acquisition phase. Throughout

[236] Department of Justice, Office of the Inspector General, The Federal Bureau of Investigation's Management of the Trilogy Information, 28.

the development period from 2001 to 2005, the FBI struggled to develop an enterprise architecture that tied the project to the agency's operational objectives. The enterprise architecture, which should have happened in the Need phase in the Acquisition Life cycle, did not happen until 2005. The VCF project's operational requirements and objectives were not well defined and the requirements kept changing after the project had started. In addition, with the weak business process change, poor leadership, and lack of expertise, the VCF project was doomed to fail in the first attempt with SAIC. Despite the initial failure and the decade spent on it, the VCF project with the name changed to Sentinel continued to completion in 2011.

VI. CONCLUSION

Large government IT projects are often categorized as high-risk and likely to fail. They are complex and take longer than two years to develop. Government IT projects are usually built to connect to multiple agencies. These projects affect a wide range of agencies' operational missions and the different types of services that these agencies provide to the public. The four government IT projects this thesis analyzed—DHS TRIO, USCG IHiS, HealthCare.gov, and FBI VCF—are categorized as large projects.[237] The challenges in the cases reviewed in this thesis are not unique. The initial failures and missteps that emerged in the case studies are not isolated cases: these issues have happened to other government projects as well. The case studies and lessons learned in this thesis may contribute to more effective practices in future large government IT projects. This chapter first presents the findings of why large IT projects fail. Second, it provides recommendations to the USCG and to large IT government acquisition projects on avoiding common mistakes and successfully implementing these projects. Third, it gives recommendations for further research to learn more from previous large IT project failures in both the government and the private sector.

A. FINDINGS

The projects explored in the four case studies all experienced schedule delays and cost increases. The DHS TRIO and HealthCare.gov projects required significant rework while IHiS and FBI VCF were cancelled and restarted as new projects. The DHS TRIO project costs increased by 54 percent from the original estimate and delayed the scheduled delivery by more than two years.[238] The USCG IHiS spent over $56 million, and after five years, it was cancelled and restarted as a completely new project named DOD MHS GENESIS.[239] The HealthCare.gov cost increased from the original estimate of $292

[237] According to the 2014 Standish report, large IT projects have budgets over $10 million and take over two years to develop, which was the case of all four case studies.

[238] Khan, DHS Financial Management: Improved Use.

[239] Powner, *Coast Guard Health Records*; "MHS GENESIS."

million to $2.1 billion.[240] The FBI wasted $105 million by the time the project was cancelled and restarted as a new project in 2005.[241] A summary of the money and time invested in the case studies' IT projects is provided in Table 5.

Table 5. Case Studies, Schedule Delays, and Cost Increases

Project	**DHS TRIO**[242]	**USCG IHiS**[243]	**HealthCare.gov**[244]	**FBI VCF**[245]
Years invested in projects before being cancelled/ restarted	More than Two Years	Five Years	Three Years	Five Years
Estimated cost	$79.2 million	$14 million	$292 million	$378 million
End cost	$122 million	$56 million	$2.1 billion	$170 million
Unusable/ Waste Cost	N/A	$56 million	N/A	$105 million
Cost increase percentage	54%	300%	619%	N/A
Result of project	Reworked	Restarted	Reworked	Restarted

240 Wayne, "Obamacare website Costs."

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

242 Khan, DHS Financial Management: Better Use.

243 Powner, Coast Guard Health Records.

244 Melvin, Health Care.Gov: CMS Has Taken Steps.

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

This thesis identifies four common causes for the failure of the four case studies' large federal IT projects. First, the projects were likely to fail when they did not define the project outcomes and/or failed to define how the outcomes would support the organizations' missions. Second, the projects often failed because they did not have the right expertise in engineering, project management, and procurement. Third, they lacked leadership support through business process change. Lastly, leadership's weak commitment to following the acquisition's progress and milestone review procedures resulted in project delays and increased costs.

1. Defining Project Outcomes at The Beginning

One reason the case studies' IT projects failed is the agencies' inability to complete the first and the most crucial step in the acquisition process: defining the project requirements. In the first case study, the DHS TRIO project, it was a year after the project transitioned to the Obtain phase (the third phase in the Acquisition Life cycle process) when DHS determined that it had not identified all of the requirements in the first two acquisition phases, the Need and Analyze/Select Phases. DHS did not fully capture how the new financial management system would interface with its other systems such as human resource and procurement systems.[246] In addition, DHS did not develop the concept of operations (CONOPS) document for the project.[247] The CONOPS document lays out how the new financial system would support the DHS mission. It also details how the new financial system would help the agency to report their financial transactions that support DHS's multiple strategic missions and comply with all of the government updated cyber security requirements. DHS TRIO should have had the CONOPS for the new financial system in the first acquisition phase, the Need phase. Missing the CONOPS caused the project to incur cost increases and schedule delays.

The second and third cases, USCG IHiS and the HealthCare.gov also did not identify all the systems' needs in the Need phase. Without identifying all the system requirements in this phase, the USCG could not validate alignment between the project

[246] Khan, DHS Financial Management: Better Use.

[247] Khan.

requirements with the USCG's health care system's operational missions. Similarly, the Centers for Medicare & Medicaid Services (CMS) could not lockdown the project requirements and scope for the HealthCare.gov website before moving into the Development and Implementation phase. This delay was due to conflicting interpretations and debates about policy around the ACA.[248] While the HealthCare.gov requirements and scope were outside of the hands of the software developers, the project still suffered from the failure to establish a clear goal and requirements in the initial phases.

Finally, in the fourth case study, the FBI VCF, the FBI also did not lock down the agency's requirements for the project in the first phase of the acquisition process. There were no well-defined requirements or CONOPS, explaining how the VCF would support FBI missions or meet operational, security, and users' objectives.[249] In other words, the FBI failed to capture what and how the VCF would help the agency's agents to perform their daily work. In each of these cases, the failure to define the project's requirements caused schedule delays and, therefore, cost increases.

All four case studies demonstrate the importance of defining requirements at the beginning of the acquisition process. Without defining the project requirements, projects are destined to fail because they lack well-defined goals, clarity on how they will add value to the organization's business, and certainty as to whether the organization needs the projects in the first place. In addition, when the projects' requirements are not defined early in the first acquisition phase, there is very high possibility that it will result in cost increase and schedule delayed as evidenced by the case studies.

2. Right Expertise

Another reason why the projects associated with the four case studies failed was a lack of the right expertise to support the projects. Some projects were unable to fill all the required vacancies to support the projects. In the DHS TRIO project, the support team, DOI-IBC, did not have the right expertise in engineering and information technology,

[248] Melvin, Health Care.Gov: CMS Has Taken Steps.

[249] Goldstein, "Who Killed the Virtual Case File?"

especially for the Oracle version 12.2 that DHS chose as the main software for the new financial management system. The HealthCare.gov contract support team MarkLogic also lacked expertise in using a nontraditional SQL platform. In both case studies, the government decided to use a newer version of the Oracle software and nontraditional SQL platform[250] instead of the older version of Oracle and the traditional SQL platform. The current staff would have needed experience in these newer versions to meet the project requirements. The lack of expertise with newer technology caused issues for the projects. This error reinforces guidance to not modify COTS products because in doing so, the seller must deviate from their core competency, potentially causing maintenance problems.[251] Specifically, in the TRIO and the HealthCare.gov cases, the IT specialists were not familiar with the new requested versions and were unable to fulfill their deliverables.

The lack of expertise was exacerbated by high rates of staff turnover in these projects as it reduced the expertise needed for their successful completion. The TRIO project experienced high staff turnover and could not fill all the required job vacancies. Unfortunately, the lack of required expertise eventually resulted in DHS cancelling the project with DOI-IBC in 2017. IHiS suffered from change in management staff,[252] which contributed to the project's failures. The project lost leadership champions, mentors, and project knowledge through the turnover. As a result, the loss of leaders negatively impacted the support staff's morale. In the HealthCare.gov project, there was a significant turnover rate of key leadership positions. The high turnover rate affected the productivity in the project because staff were overworked and stressed out.[253] Consequently, the support level for the project was negatively affected. Furthermore, the high turnover rate reduced the organizational knowledge and relationships among staff that was much needed for the HealthCare.gov project's success. Similarly, in the FBI VCF case study, the program experienced high turnover in key positions. VCF went through so much turnover in key

[250] Khan, DHS Financial Management: Better Use, 31; Levinson, HealthCare.Gov: CMS Management, 24.

[251] Blanchette, "Pros and Cons of Using COTS Products."

[252] Powner, Coast Guard Health Records.

[253] Levinson, HealthCare.Gov: CMS Management, 51.

positions that the program lost its continuity, program experience, and corporate knowledge.[254]

Expertise is essential to project development but technology advances and turnover can derail an IT acquisition project. Because government acquisition projects take a long time to develop, by the time the project is nearing completion, technology will have likely advanced. This may tempt the program office to implement the newer technology in the current acquisition project. However, this can cause problems with implementation because there are not enough IT specialists or engineers familiar with the newer technology. Consequently, the program office may have a hard time filling the positions to modify the technology to meet the project's needs. Moreover, having the right expertise and a stable team with a low turnover rate is an asset for any project. Turnover results in a loss of knowledge, continuity, and morale while the stress level for the remaining team members increases. Moreover, for new hires, the learning curve is sharper the later they join the project.[255] Therefore, it is likely turnover will escalate in environments where there is limited support and a lack of expertise.[256] In sum, high turnover has detrimental effects on team productivity.

3. Leadership Through Business Process Change

Another contributing factor to IT project failure was the lack of leadership support through business process change. Leadership is supposed to provide strong support for the project through changing communication, developing training programs, creating a user manual, and helping employees buy in to the new IT system. In the DHS TRIO project, DHS had failed to prepare for change management by not involving all the stakeholders in the buy-in process and not helping the stakeholders understand how the new system would operate.[257] In the USCG IHiS project, the USCG did not execute business process change. For instance, there was not enough training developed for the USCG or State Department

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

255 Abdel-Hamid, "A Study of Staff Turnover."

256 H.R., DHS Financial Systems, 21; Levinson, HealthCare.Gov: CMS Management, 51.

257 Khan, DHS Financial Management: Improved Use, 8.

health care workforce to get ready for the roll-out of IHiS.[258] In addition, the USCG did not develop a user manual that would help the users gain familiarity with the new health care system. Training and the user manual creation should have been taking place before the project was cancelled because, by this time, the IHiS project was already in the Obtain phase, the third acquisition phase. In this phase, the business process change should have been executed. However, due to the project's issues with undefined requirements, late attempts at establishing them could be a reason appropriate business process change was also delayed. The FBI VCF also experienced insufficient support in the user testing and vetting process. The FBI did not invest in getting the users familiar with the new VCF system, did not help the users learn how to use the system, and did not seek the users' buy-in.

Change is a challenge. Business process change helps an organization successfully transition to a new IT system. Without effective business process change an IT project will not be able to add value to the organization because employees are more likely to resist the transition and see little value added to their day-to-day operations. Regarding increasing costs and schedule delays, business process change is also designed with the user in mind. Without the users' participation in the testing process, the program may not be able to detect system errors or whether the system works as designed for the user. Consequently, the project could be cancelled due to it not meeting users' needs.

4. Leadership Through Internal Control Procedures

Leadership plays an important role to track the acquisition progress and milestone review procedures. However, as this thesis finds, faulty leadership was another reason for the failure of the IT projects. Indeed, in the IHiS project, the Coast Guard did not follow all the required steps in the System Development Life Cycle (SDLC) project management practice.[259] The process includes acquisition decision events (ADE) and milestone review procedures. Skipping these key procedures allowed the project to move forward before it was ready to do so, which can result in project failure at a later stage of the acquisition

[258] Powner, Coast Guard Health Records.

[259] Powner.

process. In the HealthCare.gov project, CMS management did not apply management tools such as progress reviews throughout the Acquisition Life cycle to monitor the project's progress, which protects the project from failures. In sum, management in both the IHiS and the HealthCare.gov projects did not provide oversight over their projects to the extent that they were supposed to.[260] The progress reviews are designed to keep the project on the right track for development purposes. Lacking leadership support through the progress review can cause negative consequences for the acquisition projects. Progress review is a management tool and is also an internal control and risk management tool. Without using the progress review properly, leadership would lose the visibility on the true progress of the project. In addition, leadership would not be able to assess whether the project's current progress would lead it to meet the designed requirements, cost and schedule. In sum, without the proper progress review, leadership would not able to do any risk mitigations to save the project from failing until it is too late.

The four large government IT projects, DHS TRIO, USCG IHiS, HealthCare.gov, and FBI VCF, shared similar results. They all experienced significant schedule delays and cost increases, which inevitably led them to fail. The major factors that contributed to the four projects' failures were not defining the project outcomes at the beginning of the Acquisition Life cycle, the lack of right expertise, and weak leadership through the business process change and the internal control procedures. The projects' challenges and shortcomings led to lessons learned in these four areas for future government and private sector large IT projects.

B. RECOMMENDATIONS

In line with the findings, this thesis provides the USCG with recommendations on how to meet IT projects' cost estimates and schedules, increase the likelihood of procuring a system that will meet its financial and operational needs, and acquire the value that the agency has paid for. The recommendations provided are applicable to any large IT acquisition project. The four case studies that this thesis reviews boil down to a few

[260] Powner, Coast Guard Health Records; Melvin, Health Care.Gov: CMS Has Taken Steps.

important elements that contribute to successful projects, especially government IT projects. These elements are defining the project outcomes at the beginning, having the right expertise, leading the organization through business process change, and fostering internal control procedures.

1. Defining Project Outcomes at the Beginning

Before an organization starts with any acquisition project, it should put together a case study to identify the organization's operational needs, and figure out whether their current system capabilities meet their needs or whether gaps exist. The findings of this case study will help develop a CONOPS and determine how the new information system would add value to the organization and how it would help the organization to carry out its operational missions or conduct its daily business.

Essentially, an organization should put together the CONOPS document in the first phase of the acquisition process. The CONOPS is not only important for the daily business but it is also a business management tool. It helps organizations with strategic and operational plans. Through the CONOPS, the organization then defines the scope and the project requirements in the Need phase.

In addition, government agencies should complete the AoA study and the market research in the Analyze/Select Phase, the second phase of the Acquisition Life cycle process. It is crucial that IT projects of the USCG, or the government in general, stay within the project scope and follow the details of the work breakdown structure.

2. Right Expertise

Leadership should commit their full support to the acquisition project by investing in human resources, such as by hiring and retaining in-house staff with all the required expertise in the areas of engineering, project management, financial management, and procurement. In addition to these areas, some projects may also require expertise in law and policy. When a project is fully staffed with all required skills and expertise, the workload can be evenly distributed and it is less stressful for the staff. The working environment for the staff is less complicated. In this condition, the team is considered to

be mature and the result is that the team will be more likely to work together successfully to support the project.

In addition, the government should be very careful when choosing a new technology or newer versions of current software. The government should verify the technology is widely available and that there is sufficient expertise in the field to fulfill the deliverables.

3. Leadership Through Business Process Change

For a project to get implemented successfully, agencies need strong support from senior management and active participation from both senior management and all the stakeholders. Program management officials, stakeholders and the project support staff must maintain a strong communication channel with each other.

Leadership should foster a partnership environment among all employees whose jobs are affected by the new system, and should have those employees involved with the program throughout the whole life cycle acquisition process. Employees who will be users of the new system should participate in defining the requirements, conducting the gap analysis, developing a case study process for the project requirements, decision making, testing and training. By providing this type of support, the leadership helps users and organizations come together as "one team" to transition smoothly to the new system. Moreover, users' participation plays a crucial role in a project's success. Especially, the participation of end users in testing a system's functionality and general testing before transitioning the system to the Operation and Maintenance phase is extremely important for the IT project. It adds value to the end users, which in turn adds value to the organization's business.

4. Leadership Through Internal Control Procedures

Lastly, leadership support must also be reflected in commitment to following the progress and milestone reviews. These types of reviews are set up as a management tool or sometimes as an internal control process to mitigate risks in acquisition projects. The reviews are intended for the leadership to review and monitor project progress and to

intervene if necessary to prevent cost increases, schedule delays, or ultimately project failures. It is imperative that leadership fully commits to participating in progress reviews as they are intended.

In summary, if the United States Coast Guard has well-defined project requirements established early in the Acquisition Life cycle; qualified staff; strong engagement from management, stakeholders, and end users; and executes timely progress reviews, the United States Coast Guard will meet the cost and schedule of an IT acquisition, but more importantly, the agency will be able to implement a successful IT system. Furthermore, the new system will meet USCG financial and operational needs. IT acquisition projects that follow the necessary steps in defining requirements, hiring and retaining qualified staff, having strong management and stakeholder engagement, having a strong business change process, and committing to following progress reviews could save the USCG millions of dollars and years of unsuccessful efforts.

C. FUTURE RESEARCH

The findings from the four case studies are derived from a small sample size which only included recent IT projects in the United States—which represents a limitation of this thesis.[261] Future research could expand on the reasons for failures of other countries' government IT and private IT projects. Future research can also focus on the lessons learned from the failures to benefit both public and private IT development projects.

[261] Another limitation to this study was not having access to all For-Official-Use-Only and sensitive documentation that might provide insight as to why such decisions in the IT acquisition projects were made. Use of open source material did not reveal insights into why leadership did not perform specific tasks.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abdel-Hamid, Tarek K. "A Study of Staff Turnover, Acquisition, and Assimilation and Their Impact on Software Development Cost and Schedule." *Journal of Management Information Systems* 6, no. 1 (1989): 21–40.

Allen, Arthur. "Coast Guard Docs Return to the Age of Paper." *Politico Morning EHealth* (blog), April 22, 2016. https://www.politico.com/tipsheets/morning-ehealth/2016/04/coast-guard-docs-return-to-the-age-of-paper-hhs-cyber-task-force-underway-213914.

Anthopoulos, Leonidas, Christopher G. Reddick, Irene Giannakidou, and Nikolaos Mavridis. "Why E-Government Projects Fail? An Analysis of the HealthCare.gov website." *Government Information Quarterly* 33, no. 1 (January 2016): 161–73. https://doi.org/10.1016/j.giq.2015.07.003.

Blanchette, J.R. "Pros and Cons of Using COTS Products." In *IEEE Autotestcon 2005*, 472–476. Orlando, FL: IEEE, 2005. doi: 10.1109/AUTEST.2005.1609182.

Centers for Medicare & Medicaid Services. *Guide to Enterprise Life Cycle Processes, Artifacts, and Reviews*. Version 1.1. Washington, DC: Department of Health and Human Services, 2012. https://medicaid.ms.gov/wp-content/uploads/2014/03/Appendix-K-CMS-Enterprise-Life-Cycle.pdf.

"Clinger-Cohen Act of 1996," Pub. L. No. 104–106, § Public Buildings, Property and Works, Title 40 USCODE-2011 13 (1996), https://www.govinfo.gov/content/pkg/USCODE-2011-title40/pdf/USCODE-2011-title40-subtitleIII.pdf.

Creately Blog. "Process Documentation Guide: Learn How to Document Processes." *Creately* (blog), January 29, 2018. https://creately.com/blog/diagrams/process-documentation-guide/.

Department of Justice, Office of the Inspector General. *Federal Bureau of Investigation's Management of Information Technology Investments*. Audit Report 03–09. Washington, DC: Department of Justice, Office of the Inspector General, 2002. https://oig.justice.gov/reports/FBI/a0309/final.pdf.

———. *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project*. Audit Report 05–07. Washington, DC: Department of Justice, 2005. https://oig.justice.gov/reports/FBI/a0507/final.pdf.

Donovan, Shaun. *Management and Oversight of Federal Information Technology*. M-15–14. Washington, DC: Office of Management and Budget, 2015. https://www.fai.gov/sites/default/files/2015-06-10-OMB-Memo-FITARA.pdf.

Esteves, José, and Rhoda C. Joseph. "A Comprehensive Framework for the Assessment of EGovernment Projects." *Government Information Quarterly* 25, no. 1 (January 2008): 118–32. https://doi.org/10.1016/j.giq.2007.04.009.

Fairley, Richard E., and Mary Jane Willshire. "Why the Vasa Sank: 10 Problems and Some Antidotes for Software Projects." *IEEE Software* 20, no. 2 (March 2003): 18–25. https://doi.org/10.1109/MS.2003.1184161.

Federal Acquisition Regulations. "Cost-Plus-Fixed-Fee Contracts," Title 48 (2014 comp.): 16.306 §. Electronic Code of Federal Regulation (e-CFR). Accessed September 10, 2020. https://www.govinfo.gov/content/pkg/CFR-2019-title48-vol1/pdf/CFR-2019-title48-vol1-part16.pdf.

General Services Administration. "Shared Services." Accessed April 9, 2021. https://www.gsa.gov/shared-services.

Gil-García, J. Ramón, and Theresa A. Pardo. "E-Government Success Factors: Mapping Practical Tools to Theoretical Foundations." *Government Information Quarterly* 22, no. 2 (2005): 187–216. https://doi.org/10.1016/j.giq.2005.02.001.

Goldstein, Harry. "Who Killed the Virtual Case File? [Case Management Software]." *IEEE Spectrum* 42, no. 9 (September 2005): 24–35. https://doi.org/10.1109/MSPEC.2005.1502526.

Government Accountability Office. "Antideficiency Act Resources." Accessed March 15, 2021. https://www.gao.gov/legal/appropriations-law/resources.

Guidebook for the Acquisition of Services: ACE for Services. Washington, DC: Department of Defense, 2012. https://www.acq.osd.mil/dpap/ccap/cc/corhb/files/miscellaneous_training/guidebook_for_acquisition_of_services_24march2012.pdf.

Hardy-Vallée, Benoit. "The Cost of Bad Project Management." *Business Journal*, February 7, 2012. https://news.gallup.com/businessjournal/152429/cost-bad-project-management.aspx?

Harris, Carol C. Information Technology: Implementation of GAO Recommendations Would Strengthen Federal Agencies' Acquisitions, Operations, and Cybersecurity Efforts. GAO-19-641T. Washington, DC: Government Accountability Office, 2019. https://www.gao.gov/products/GAO-19-641T.

HealthCare.gov. "Affordable Care Act (ACA)." Accessed August 17, 2020. https://www.healthcare.gov/glossary/affordable-care-act/.

Hite, Randolph C. *Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*. GAO-03-959. Washington, DC: General Accounting Office, 2003. https://www.gao.gov/assets/gao-03-959.pdf.

IEEE Computer Society. *IEEE Standard for Software and System Test Documentation*. IEEE Std 829–2008. New York: IEEE, 2008.

Imamoglu, Oksan, and Sitki Gozlu. "The Sources of Success and Failure of Information Technology Projects: Project Managers' Perspective." In *Technology Management for a Sustainable Economy*, edited by Dundar F. Kocaoglu, Timothy R. Anderson, and Tugrul U. Daim, 1430–35. Portland OR: IEEE, 2008. https://doi.org/10.1109/PICMET.2008.4599756.

Israel, Jerome. "Why the FBI Can't Build a Case Management System." *Computer* 45, no. 6 (June 2012): 73–80. https://doi.org/10.1109/MC.2012.2.

Kadish, Ronald, Gerald Abbot, Frank Cappuccio, Richard Hawley, Paul Kern, and Donald Kozlowski. *Defense Acquisition Performance Assessment Report*. Washington, DC: Assessment Panel of the Defense Acquisition Performance Assessment Project, 2006. https://apps.dtic.mil/dtic/tr/fulltext/u2/a459941.pdf.

Khan, Asif A. *DHS Financial Management: Better Use of Best Practices Could Help Management System Modernization Project Risk*. GAO-17-799. Washington, DC: Government Accountability Office, 2017. https://www.gao.gov/assets/690/687362.pdf.

———. *DHS Financial Management: Improved Use of Best Practices Could Help Manage System Modernization Project Risks.* Testimony Before the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives. GAO-17-803T. Washington, DC: Government Accountability Office, 2017. https://www.gao.gov/assets/690/687359.pdf.

Landi, Heather. "U.S. Coast Guard Terminated Contract with Epic for EHR Implementation." *Healthcare Innovation*, April 25, 2016. https://www.hcinnovationgroup.com/policy-value-based-care/news/13026683/us-coast-guard-terminated-contract-with-epic-for-ehr-implementation.

Levinson, Daniel R. *HealthCare.gov : CMS Management of the Federal Marketplace: A Case Study*. OEI-06-14-00350. Washington, DC: Department of Health and Human Services, 2016. https://oig.hhs.gov/oei/reports/oei-06-14-00350.pdf.

Lohrmann, Dan. "Why Do Many Big IT Projects Fail in Government?" *Lohrmann on Cybersecurity* (blog), November 3, 2013. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/Why-do-many-big-IT-projects-fail-in-government.html.

Marinaro, John. "Why Federal IT Projects Fail (and How to Ensure Success)." *Nextgov*, March 11, 2019. https://www.nextgov.com/ideas/2019/03/why-federal-it-projects-fail-and-how-ensure-success/155435/.

Mark, Marie A. Amphibious Combat Vehicle: Some Acquisition Activities Demonstrate Best Practices; Attainment of Amphibious Capability to Be Determined. GAO-16-22. Washington, DC: Government Accountability Office, 2015. https://www.gao.gov/assets/gao-16-22.pdf.

McFarlan, F. Warren. "Portfolio Approach to Information Systems." *Harvard Business Review* 59, no. 5 (September 1981): 142–50.

McGroddy, James C., and Herbert S. Lin, eds. *A Review of the FBI's Trilogy Information Technology Modernization Program*. Washington, DC: National Academies Press, 2004. https://doi.org/10.17226/10991.

Michel, Charles D. ADM. "Financial Management Service Improvement Initiative (FMSII) Program Breach Notification." Official memorandum. Washington, DC: United States Coast Guard, 2017.

Melvin, Valerie C. *Health Care.Gov: CMS Has Taken Steps to Address Problem, but Needs to Further Implement System Development Best Practices.* GAO-15-238. Washington, DC: Government Accountability Office, 2015. https://www.gao.gov/assets/670/668834.pdf.

Military Health System. "MHS GENESIS." Accessed April 9, 2021. https://www.health.mil/Military-Health-Topics/Technology/Federal-Electronic-Health-Record-Modernization/MHS-GENESIS.

Mihm, J. Christopher, and Robert Goldenkoff. *Government Reorganization: Key Questions to Assess Agency Reform Efforts*. GAO-18-427. Washington, DC: Government Accountability Office, 2018. https://www.gao.gov/assets/gao-18-427.pdf.

Mueller, Robert S. III. "Testimony. FBI's Virtual Case File System." Federal Bureau of Investigation web archive. Accessed August 29, 2021. https://archives.fbi.gov/archives/news/testimony/fbis-virtual-case-file-system.

Nielsen, Jeppe Agger, and Keld Pedersen. "IT Portfolio Decision-Making in Local Governments: Rationality, Politics, Intuition and Coincidences." *Government Information Quarterly* 31, no. 3 (July 2014): 411–20. https://doi.org/10.1016/j.giq.2014.04.002.

Office of Management and Budget. *Guidelines and Discount Rates for Benefits-Cost Analysis of Federal Programs*. OMB Circular A-94. Washington, DC: Office of Management and Budget. Accessed April 23, 2021. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A94/a094.pdf.

———. *Financial Management Systems*, interim final revision of OMB Circular A-127. Washington, DC: Office of Management and Budget, 1999. https://www.whitehouse.gov/wp-content/uploads/2017/11/Interim-Final-Revision-of-OMB-Circular-A-125-July11999.pdf.

———. "Our Information Technology Investments at Work," *ITDashboard.gov*. Accessed August 29, 2021. https://myit-2019.itdashboard.gov/.

Office of the Auditor General of Canada. *Report 1—Building and Implementing the Phoenix Pay System*. Ottawa, Ontario: Reports of the Auditor General of Canada, May 29, 2018. http://www.oag-bvg.gc.ca/internet/English/att__e_43045.html.

Oracle. "What Is a Database?" Accessed May 10, 2021. https://www.oracle.com/in/database/what-is-database/.

Payne, Adam. "80% of Major Government Projects Are at 'Risk of Failure' as Civil Servants Struggle to Cope with Brexit." *Business Insider*, January 25, 2018. https://www.businessinsider.com/ifg-report-major-government-projects-at-risk-of-failure-brexit-2018-1.

Persons, Timothy M. *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*. GAO-20-195G. Washington, DC: Government Accountability Office, 2020. https://www.gao.gov/assets/gao-20-195g.pdf.

Powner, David A. *Coast Guard Health Records: Timely Acquisition of New System Is Critical to Overcoming Challenges with Paper Process*. GAO-18-59. Washington, DC: Government Accountability Office, 2018. https://www.gao.gov/assets/690/689565.pdf.

Project Management Institute, Inc. *Managing Change in Organizations: A Practice Guide*. Newtown Square, PA: Project Management Institute, Inc., 2013.

Riotta, Chris. "GOP Aims to Kill Obamacare Yet Again after Failing 70 Times." *Newsweek*, July 29, 2017. https://www.newsweek.com/gop-health-care-bill-repeal-and-replace-70-failed-attempts-643832.

Sarantis, Demetrios, Yannis Charalabidis, and Dimitris Askounis. "A Goal-Driven Management Framework for Electronic Government Transformation Projects Implementation." *Government Information Quarterly* 28, no. 1 (January 2011): 117–28. https://doi.org/10.1016/j.giq.2009.10.006.

Streett, Bryant. *Analysis of Alternatives (AoA) Methodologies: Considerations for DHS Acquisition Analyses, Version 3.0*. RP13-01.04.05-01. Falls Church, VA: Homeland Security Studies and Analysis Institute, 2014. https://www.anser.org/docs/reports/AOA%20Methodologies%20Considerations%20for%20DHS%20Acq%20Analysis.pdf.

The Standish Group. *CHAOS Report: 21st Anniversary Edition*. West Yarmouth, MA: The Standish Group International, Inc., 2014. https://www.standishgroup.com/sample_research_files/CHAOSReport2014.pdf

———. *CHAOS Report 1995*. West Yarmouth, MA: The Standish Group International, Inc., 1994. https://www.researchgate.net/publication/263849222.

———. *CHAOS Report 2004*. West Yarmouth, MA: The Standish Group International, Inc., 2003. http://blog.nalis.fr/public/pdf/q3-spotlight.pdf.

———. *Extreme CHAOS*. West Yarmouth, MA: The Standish Group International, Inc., 2001. https://courses.cs.ut.ee/MTAT.03.243/2013_spring/uploads/Main/standish.pdf.

Thompson, K. "Supreme Court Ruling on the Affordable Care Act." *NAFC, The National Association of Free & Charitable Clinics* (blog). November 10, 2020. https://www.nafcclinics.org/content/supreme-court-ruling-affordable-care-act.

Trimble, David C. *DOE and NNSA Project Management: Analysis of Alternatives Could Be Improved by Incorporating Best Practices*. GAO-16-37. Washington, DC: Government Accountability Office, 2014. https://www.gao.gov/assets/670/667404.pdf.

U.S. Coast Guard. "ALCOAST 091/18 - Mar 2018 Financial Management and Procurement Services Modernization - Update 2." U.S. Coast Guard, March 14, 2018. https://content.govdelivery.com/accounts/USDHSCG/bulletins/1e206d1.

———. "Coast Guard Operational Assets." United States Coast Guard. Accessed April 30, 2021. https://www.uscg.mil/About/Assets/.

———. "Missions." United States Coast Guard. Accessed April 30, 2021. https://www.uscg.mil/About/Missions/.

———. *USCG System Development Life Cycle (SDLC) Practice Manual, Revision 4.0*. SDLC Product #107. Washington, DC: U.S. Coast Guard, 2011. https://cg.portal.uscg.mil/communities/sdlc--pprb--pprb-wg/SDLC/LIBRARY/PRODUCTS/PRACTICE/Current%20Final.pdf.

U.S. Coast Guard Acquisition Directorate. "Electronic Health Records Acquisition." Accessed August 24, 2020. https://www.dcms.uscg.mil/Our-Organization/Assistant-Commandant-for-Acquisitions-CG-9/Programs/C4ISR-Programs/Electronic-Health-Records-Acquisition/.

———. *Level 3 Non-Major Acquisition Program (NMAP) Manual*. COMDTINST M5000.11C. Washington, DC: U.S. Coast Guard Acquisition Directorate, June 5, 2019. https://media.defense.gov/2019/Jun/12/2002144388/-1/-1/0/CIM_5000_11C.PDF.

———. *Major Systems Acquisition Manual (MSAM)*. COMDTINST M5000.10A, Version 2.1. Washington, DC: U.S. Coast Guard Acquisition Directorate, March 16, 2009. https://www.hsdl.org/?view&did=22315.

Wayne, Alex. "Obamacare website Costs Exceed $2 Billion, Study Finds." *Bloomberg*, September 24, 2014. https://www.bloomberg.com/news/articles/2014-09-24/obamacare-website-costs-exceed-2-billion-study-finds.

Werfel, Danny. "Improving Financial Systems through Shared Services," Memorandum for the heads of executive departments and agencies. M-13-08. Washington, DC: Office of Management of Budget, March 25, 2013. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2013/m-13-08.pdf.

Yaraghi, Niam. "Doomed: Challenges and Solutions to Government IT Projects." *TechTank* (blog), August 25, 2015. https://www.brookings.edu/blog/techtank/2015/08/25/doomed-challenges-and-solutions-to-government-it-projects/.

Young, Chuck. *Information Technology: Investment Management: An Overview of GAO's Assessment Framework*. GAO/AIMD-00-155. Washington, DC: General Accounting Office, 2000. https://www.gao.gov/products/aimd-00-155.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California