NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

BUILDING AUTOMATION SYSTEM CYBER NETWORKS: AN UNMITIGATED RISK TO FEDERAL FACILITIES

by

Shawn P. Tupper

December 2015

Thesis Advisors: Kathleen Kiernan
John Rollins

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2015	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE BUILDING AUTOMATION SYSTEM CYBER NETWORKS: AN UNMITIGATED RISK TO FEDERAL FACILITIES			**5. FUNDING NUMBERS**
6. AUTHOR(S) Shawn P. Tupper			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The General Services Administration accesses building-automation system technology that runs federal facility processes such as HVAC, lighting, elevators, and access control via active Internet connections. Currently, these networks are not secure, despite legislation requiring them to be.

This thesis investigated whether the Department of Homeland Security (DHS) could leverage existing federal laws, presidential directives, executive orders, government frameworks, and its current cyber and investigative capabilities to establish a strategy to secure federal facility building-automation system cyber networks, or if additional resources are needed The research uncovered significant vulnerabilities and threats to federal facility building-automation system networks, which, if exploited, could cause a significant impact on the American people, who are dependent on services offered by federal agencies such as the Department of Veterans Affairs and the Social Security Administration.

A qualitative research method was used to interpret and analyze government and nongovernment institutional studies and reports, existing cybersecurity frameworks, and scholarly journals to determine which of the policy options offered would provide the best strategy for the DHS moving forward. The thesis concluded that utilizing a combination of private contractors and existing DHS assets would provide the best option.

14. SUBJECT TERMS industrial control systems, building automation systems, cybersecurity, Federal Protective Service (FPS), United States Secret Service (USSS), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), General Services Administration (GSA), Shodan, EINSTEIN, CSET, DHS, Department of Homeland Security			**15. NUMBER OF PAGES** 131
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

BUILDING AUTOMATION SYSTEM CYBER NETWORKS: AN UNMITIGATED RISK TO FEDERAL FACILITIES

Shawn P. Tupper
Senior Special Agent, U.S. Department of Homeland Security
B.A., American Military University, 2006

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
December 2015**

Approved by: Kathleen Kiernan, Ph.D.
Thesis Co-Advisor

John Rollins
Thesis Co-Advisor

Erik Dahl,
Associate Chair for Instruction,
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The General Services Administration accesses building-automation system technology that runs federal facility processes such as HVAC, lighting, elevators, and access control via active Internet connections. Currently, these networks are not secure, despite legislation requiring them to be.

This thesis investigated whether the Department of Homeland Security (DHS) could leverage existing federal laws, presidential directives, executive orders, government frameworks, and its current cyber and investigative capabilities to establish a strategy to secure federal facility building-automation system cyber networks, or if additional resources are needed The research uncovered significant vulnerabilities and threats to federal facility building-automation system networks, which, if exploited, could cause a significant impact on the American people, who are dependent on services offered by federal agencies such as the Department of Veterans Affairs and the Social Security Administration.

A qualitative research method was used to interpret and analyze government and nongovernment institutional studies and reports, existing cybersecurity frameworks, and scholarly journals to determine which of the policy options offered would provide the best strategy for the DHS moving forward. The thesis concluded that utilizing a combination of private contractors and existing DHS assets would provide the best option.

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

BAS	Building Automation Systems
CEA	Cybersecurity Enhancement Act of 2002
CERT	computer emergency response team
CFAA	Computer Fraud and Abuse Act
CFS	Commercial Facilities Sector
CI	Critical Infrastructure
CIKR	critical infrastructure and key resources
CIO	chief information officer
CRS	Congressional Research Service
CS&C	Office of Cybersecurity and Communications
CSET	Cyber Security Evaluation Tool
CSP	Critical Systems Protection Program
CSSP	Control Systems Security Program
CWAA	Cybersecurity Workforce Assessment Act of 2014
DBT	Design-Basis Threat
DHS	Department of Homeland Security
DHS-OIG	DHS Office of Inspector General
DOD	Department of Defense
DOE	Department of Energy
EO	Executive Order
FISMA	Federal Information Security Management Act
FPS	Federal Protective Service
GAO	Government Accountability Office
GFS	Government Facilities Sector
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
ICS	industrial control system
ICS-CERT	Industrial Control System Cyber Emergency Response Team
IDS	intrusion detection system
IP	Infrastructure Protection

IPS	intrusion prevention system
ISC	Interagency Security Committee
IT	information technology
MOA	memorandums of agreement
NCCIC	National Cybersecurity and Communications Integration Center
NCIJTF	National Cyber Investigative Joint Task Force
NCPA	National Cybersecurity Protection Act
NICE	National Initiative for Cybersecurity Education
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
NSA	National Security Agency
NSPD	National Security Presidential Directive
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OT	operational technology
PBS	Public Building Service
PII	personally identifiable information
PSO	protective security officer
SSA	supervisory special agent

EXECUTIVE SUMMARY

In 2007, Congress passed the Energy Independence and Security Act, directing all government agencies to reduce their buildings' energy levels by 30 percent by 2015.[1] Accordingly, the General Services Administration (GSA), responsible for managing federal facilities, began taking the necessary steps to accomplish this goal.[2] In 2012, to reduce energy costs and improve performance, GSA began retrofitting 50 of the most energy-inefficient federal facilities.[3] This retrofit included networking facility building automation systems (BAS)—a type of industrial control system (ICS) to the Internet—to give "property managers real-time information and diagnostic tools that keep facilities working at peak efficiency."[4] These BAS networks control such actions as HVAC, facility lighting, and elevators.[5] Although this technology has created both a centralization of control and a level of convenience for GSA property managers and building engineers, allowing them to perform facility maintenance from the click of a mouse, it has also made the facilities vulnerable to cyber intrusions due to their active Internet connections.

Currently, the Department of Homeland Security (DHS) is not monitoring BAS networks, investigating network intrusions, or conducting risk assessments of BAS networks inside GSA-owned facilities, despite current presidential executive orders (E.O.s) and federal laws such as the Federal Information Security Management Act of 2002 (FISMA), requiring federal networks be secured.[6] DHS and the GSA are the agencies responsible for the Government Facilities Sector (GFS), one of the 16 critical

---

[1] *Energy Independence and Security Act of 2007*, Pub. L. No. 110–140 Stat. 1596 (2007)

[2] *Federal Green Buildings, U.S. House of Representatives*, 111th Cong., (statement by Kevin Kampschroer, Director Office of Federal High-Performance Green Buildings).

[3] "New Smart Building Technology to Increase Federal Buildings Energy Efficiency," General Services Administration, May 12, 2012, http://www.gsa.gov/portal/content/135115.

[4] Ibid.

[5] U.S. Government Accountability Office, *Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems* (GAO-15-6) (Washington, DC: U.S. Government Accountability Office, 2014), 10, http://www.gao.gov/assets/670/667512.pdf.

[6] Ibid., 17.

infrastructure sectors outlined in the National Infrastructure Protection Plan (NIPP); the GSA is ultimately responsible for federal facility BAS security.[7]

Currently, there is insufficient collaboration within the DHS with respect to securing federal facility BAS networks, despite well-known threats and vulnerabilities such as password-management deficiencies, unsubstantial intrusion detection, and inferior private-sector network monitoring.[8] Though the reason for the DHS's lack of collaboration is unknown, it may be because the Department has not yet seen that these networks operating in federal facilities are susceptible to penetration and subsequent exploitation. This has likely led to poor motivation within the DHS and GSA to address the issue. Other potential factors could be limited resources—no trained personnel and budget constraints—and confusion related to jurisdiction or authority. Finally, existing federal laws, presidential EOs, and cybersecurity frameworks may not be sufficient to provide the necessary roadmap for collaboration between federal agency stakeholders to secure federal facility BAS networks.

There are both tangible and intangible consequences related to a cyberattack upon a federal facility BAS. First, disruption in HVAC, lighting, or elevator operations could cause facility closure until the problem is resolved, creating a backlog for government entitlement agencies such as the Social Security Administration and the Department of Veterans Affairs. Second, if the HVAC system were tampered with, increasing temperatures in the facility could render individual agencies' network servers inoperable or, worse, could cause health and safety concerns for the young and elderly. Third, if an attacker surreptitiously enters a BAS network, the attacker could subsequently gain access to the GSA.gov network, potentially compromising personally identifiable information (PII) of GSA customers (the rest of the federal government). Finally, if a federal facility BAS network attack became public, confidence in government would

---

[7] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (NIPP 2013) (Washington, DC: U.S. Department of Homeland Security, 2013), 8, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

[8] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 22.

likely be further eroded; A June 2014 Gallup poll found that more than 70 percent of the American people have already lost confidence in the federal government.[9]

This thesis examines current legislation and DHS cyber capabilities, and answers the primary research question:

- How can the DHS leverage existing federal laws, presidential directives, executive orders, and frameworks, and its current cyber and investigative capabilities to establish a strategy to secure federal facility building-automation system networks?

The following secondary research questions are answered to properly address the primary research question:

- If existing resources are not sufficient, what additional resources should be obtained to mitigate the risks?
- How should the DHS leverage its components' law enforcement authorities to augment technical cyber defense measures?

The current DHS strategy to secure federal facility BAS is nonexistent; however, both the DHS and GSA have recently agreed to work together to develop a strategy.[10] There are many challenges associated with increasing cybersecurity within the federal government, and specifically within cybersecurity of federal facility BAS networks. Some challenges include determining if existing laws are sufficient to prosecute bad actors, finding the balance between security and privacy, determining roles and responsibilities for government agencies, addressing lack of trained personnel, and planning for the constantly changing nature of the threat. This thesis analyzes the current roadblocks to achieving security of BAS networks inside federal facilities, cybersecurity law and legal authorities the federal government already possesses to secure federal facility BAS networks, and the DHS and GSA responsibilities in this effort.

Perhaps the biggest roadblock to securing federal facility BAS is the DHS and GSA's lack of control over the contractors currently maintaining most BAS networks. As of March 2015, approximately three hundred federal facility BAS networks are housed

---

[9] Justin McCarthy, "Americans Losing Confidence in All Branches of U.S. Gov't," Gallup, June 20, 2014, http://www.gallup.com/poll/171992/americans-losing-confidence-branches-gov.aspx.

[10] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, Appendix III, IV.

on the GSA network, and protected behind the GSA firewall; the remaining facilities are operated on private contractor networks.[11] While GSA is in the process of moving these facilities over to their network, until this happens, these networks are essentially beyond the control of the government.

Another roadblock the DHS faces is that it does not currently have sufficient technical expertise to assess these networks on a broad scale, nor to investigate possible intrusions for eventual prosecution of bad actors, with the lone exception of the United States Secret Service (USSS).[12] The Industrial Control System Cyber Emergency Response Team (ICS-CERT) informed the author they have less than 30 personnel who are trained to respond to cybersecurity incidents of ICS networks and they lack law enforcement authority. Conversely, the Federal Protective Service (FPS) has the necessary law enforcement authority and responsibility to protect federal facilities, yet lacks the technical expertise to perform cybersecurity duties.[13] Currently, the only DHS component with both law enforcement authority to conduct criminal investigations and ICS forensic expertise is the USSS.[14] The Secret Service, however, is not currently conducting any investigative activity related to GSA-owned facility BAS network intrusions.

Five options are offered in this inquiry and were assessed using five categories: DHS acceptability, compliance (with laws and presidential executive orders and directives), ease of implementation, overall effectiveness, and time needed to implement

---

[11] Josh Mordin and Sandy Schadchehr, "Building Monitoring and Control Systems in GSA," presented at the Cybersecurity Building Control Systems Workshop, Washington, DC, March 24, 2015

[12] Senate Committee on Appropriations, Subcommittee on Homeland Security, *Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future* (statement by Special Agent in Charge William Noonan, May 7, 2014.

[13] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 5, 18.

[14] *Fighting Fraud: Improving Information Security: Joint Hearing Before the House Subcommittee on Financial Institutions And Consumer Credit of the Committee on Financial Services*, 108th Cong., 1(2003) (statement of Tim Caddigan, Special Agent in Charge, Financial Crimes Division, United States Secret Service).

the option.[15] A subsequent comparative analysis was completed to discover which option earned the highest ratings.

The comparative analysis findings demonstrated that the DHS should adopt and implement Option IV(A) by initially utilizing experienced, cleared private contractors, overseen by FPS, to perform risk assessments and network analysis of federal facility BAS. Additionally, Option IV(A) calls for the DHS to direct the USSS to provide incident response for network intrusions, as well as subsequent forensically sound criminal investigations into the discovered intrusions. Once the FPS has established their own cybersecurity capability, the agency would be charged with taking over the mission completely. This option provides an almost immediate, cost-effective risk mitigation strategy to reduce the vulnerabilities identified in Government Accountability Office (GAO) report 15–6.

[15] Todd R. Consolini, "Regional Security Assessments: A Regional Approach to Securing Federal Facilities" (master's thesis, Naval Postgraduate School, 2009).

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my amazing wife, Dina, and our children, Sophia and Olivia, for the sacrifices they have made and the unwavering support they have given me during this journey. No more missed birthdays, anniversaries, and holidays, not to mention countless weekends at the office and library. I could not have done this without your love and patience. Thank you.

My senior leadership could not have been more supportive: Mr. Bruce Ellison and Mr. Anthony Losito of the Department of Homeland Security and Mr. Storemski of the FBI. Thank you for allowing me to travel back and forth between West Virginia and California for weeks at a time, and for approving several weeks of annual leave to get this thesis completed; your support and encouragement enabled me to get to the finish line. Thank you.

A special thanks to Mr. Consolini and Mr. Arnfeld for allowing me to test my theories, providing me reality checks, and constantly feeding me ideas to make this thesis a reality.

I would also like to thank my thesis advisors, Dr. Kathleen Kiernan and Mr. John Rollins, who allowed me to find my own way while offering support and guidance when necessary. I believe I will be relying on you for advice and counsel for years to come.

Finally, thanks to Scott Martis: What would 1403/1404 have done without you? Scott, you were the glue that bonded our class from day one, and in you each of us has made a lifelong friend. Thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In 2007, Congress passed the Energy Independence and Security Act, directing all government agencies to reduce their buildings' energy levels by 30 percent by 2015.[1] Accordingly, the General Services Administration (GSA), responsible for managing federal facilities, began taking the necessary steps to accomplish this goal.[2] In 2012, to reduce energy costs and improve performance, GSA began retrofitting 50 of the most energy-inefficient federal facilities.[3] This retrofit included networking facility building automation systems (BAS)—a type of industrial control system (ICS) to the Internet—to give "property managers real-time information and diagnostic tools that keep facilities working at peak efficiency."[4] All new federal facility construction will employ BAS network technology. These BAS networks control such actions as HVAC, facility lighting, and elevators.[5] Although this technology has created both a centralization of control and a level of convenience for GSA property managers and building engineers, allowing them to perform facility maintenance from the click of a mouse, it has also made the facilities vulnerable to cyber intrusions due to their active Internet connections.

Currently, the Department of Homeland Security (DHS) is not monitoring BAS networks, investigating network intrusions, or conducting risk assessments of BAS networks inside GSA-owned facilities, despite current presidential executive orders (E.O.s) and federal laws, such as the Federal Information Security Management Act of 2002 (FISMA), requiring federal networks be secured.[6] The DHS and GSA are designated as the co-sector-specific agencies responsible for the Government Facilities

---

[1] *Energy Independence and Security Act of 2007*, Pub. L. No. 110-140 Stat. 1596 (2007).

[2] *Federal Green Buildings, U.S. House of Representatives*, 111th Cong., (statement by Kevin Kampschroer, Director Office of Federal High-Performance Green Buildings).

[3] "New Smart Building Technology to Increase Federal Buildings Energy Efficiency," General Services Administration, May 12, 2012, http://www.gsa.gov/portal/content/135115.

[4] Ibid.

[5] U.S. Government Accountability Office, *Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems* (GAO-15-6) (Washington, DC: U.S. Government Accountability Office, 2010), 10, http://www.gao.gov/assets/670/667512.pdf.

[6] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 17.

Sector (GFS), one of the 16 critical infrastructure sectors outlined in the National Infrastructure Protection Plan (NIPP), and are ultimately responsible for federal facility BAS security.[7] The NIPP lists cybersecurity for critical infrastructure and key resources (CIKR), such as industrial control system (ICS), as a critical point of vulnerability in the U.S. industrial infrastructure.[8]

Additionally, Homeland Security Presidential Directive (HSPD)-7, superseded by PPD-21, directed the DHS to produce a national plan to protect CIKR, and designated the DHS as a national focal point for securing cyberspace.[9] To streamline this effort, the National Protection and Programs Directorate (NPPD), a subcomponent of the DHS, established the Control Systems Security Program (CSSP). The CSSP is responsible for maintaining a partnership between the federal government and private industry to reduce cyber threats to private sector BAS/ICS; this program, however, does not address federal facility BAS, leaving a significant gap in federal facility BAS network security.[10]

Currently, there is insufficient collaboration within the DHS with respect to securing federal facility BAS networks, despite well-known threats and vulnerabilities such as password-management deficiencies, unsubstantial intrusion detection, and inferior private-sector network monitoring.[11] Though the reason for the DHS's lack of collaboration is unknown, it may be because the Department has not yet seen that these networks operating in federal facilities are susceptible to penetration and subsequent exploitation. This has likely led to poor motivation within the DHS and GSA to address the issue. Other potential factors could be limited resources—limited trained personnel

---

[7] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (NIPP 2013) (Washington, DC: U.S. Department of Homeland Security, 2013), 8, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

[8] Ibid., 12.

[9] President of the United States, *Homeland Security Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection* (HSPD-7) (Washington, DC: U.S. Department of Homeland Security, 2003), http://www.dhs.gov/homeland-security-presidential-directive-7.

[10] Office of Inspector General, *DHS Can Make Improvements to Secure Industrial Control Systems* (OIG-13-39) (Washington, DC: U.S. Department of Homeland Security, 2013), 3, https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-39_Feb13.pdf.

[11] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 22.

and budget constraints—and confusion related to jurisdiction or authority. Finally, existing federal laws, presidential EOs, and cybersecurity frameworks may not be sufficient to provide the necessary roadmap for collaboration between federal agency stakeholders to secure federal facility BAS networks.

There are both tangible and intangible consequences related to a cyberattack upon a federal facility BAS. First, disruption in HVAC, lighting, or elevator operations could cause facility closure until the problem is resolved, creating a backlog for government entitlement agencies such as the Social Security Administration and the Department of Veterans Affairs. Second, if the HVAC system were tampered with, increasing temperatures in the facility could render individual agencies' network servers inoperable or, worse, could cause health and safety concerns for the young and elderly. Third, if an attacker surreptitiously enters a BAS network, the attacker could subsequently gain access to the GSA.gov network, potentially compromising personally identifiable information (PII) of GSA customers (the rest of the federal government). Finally, if a federal facility BAS network attack became public, confidence in government would likely be further eroded; A June 2014 Gallup poll found that more than 70 percent of the American people have already lost confidence in the federal government.[12]

A. EVOLUTION OF FEDERAL FACILITY SECURITY

In 1995, over one million federal employees worked in approximately 1,330 GSA-owned or leased facilities, and the numbers are remarkably similar today.[13] Before the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995, no formal security standards for federally owned or leased facilities existed.[14] In the aftermath, President Clinton charged the Department of Justice with determining if federal facilities were vulnerable to violence or terrorism, and to "develop

[12] McCarthy, "Americans Losing Confidence."

[13] United States Marshals Service, *Vulnerability Assessment of Federal Facilities* (Washington, DC: U.S. Department of Justice, 1995), Introduction, https://www.ncjrs.gov/pdffiles1/Digitization/156412NCJRS.pdf.

[14] Lorraine H. Tong, *Federal Building and Facility Security* (CRS Report No. R41138) (Washington, DC: Congressional Research Service, 2010), 1.

recommendations for minimum security standards."[15] The GSA and the U.S. Marshals Service conducted over 1,200 physical security assessments at federal facilities in order to determine what building upgrades would be necessary in order to comply with the minimum standards proposed.[16]

Recommendations such as improving access control, occupant emergency plans, and intelligence sharing were made.[17] Facilities were also grouped by security levels, ranging from V (the most secure) to I (the least secure), and minimal standards for each level were established.[18] All executive branch agencies were subsequently directed by President Clinton "to begin upgrading their facilities to meet the recommended minimum security standards."[19] The GSA was also required to "establish Building Security Committees for all of its facilities."[20] These committees meet on an as-needed basis to discuss security-related matters, such as if existing countermeasures are sufficient.

On October 19, 1995, the Interagency Security Committee (ISC) was established through Executive Order 12977.[21] The ISC was chaired by the GSA Administrator until 2003, when the chairmanship transferred to the Secretary of the DHS. E.O. 12977 charged the ISC with the responsibilities outlined in Figure 1.

---

[15] U.S. Government Accountability Office, *Building Security: Interagency Security Committee Has Had Limited Success in Fulfilling its Responsibilities* (GAO-02-1004) (Washington, DC: U.S. Government Accountability Office, 2002), 5.

[16] Tong, *Federal Building and Facility Security*, 1.

[17] United States Marshals Service. *Vulnerability Assessment of Federal Facilities*.

[18] Ibid.

[19] Tong, *Federal Building and Facility Security*, 1.

[20] Ibid.

[21] U.S. Government Accountability Office, *Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices* (GAO-05-49) (Washington, DC: U.S. Government Accountability Office, 2004).

Figure 1. ISC Responsibilities Mandated by E.O. 12977

1. Establish policies for security in and protection of Federal facilities
2. Develop and evaluate security standards for Federal facilities, develop a strategy for ensuring compliance with such standards, and oversee the implementation of appropriate security measures in Federal facilities
3. Take such actions as may be necessary to enhance the quality and effectiveness of security and protection of Federal facilities, including but not limited to:
    a. encouraging agencies with security responsibilities to share security-related intelligence in a timely and cooperative manner
    b. assessing technology and information systems as a means of providing cost-effective improvements to security in Federal facilities
    c. developing long-term construction standards for those locations with threat levels or missions that require blast resistant structures or other specialized security requirements
    d. evaluating standards for the location of, and special security related to, day care centers in Federal facilities
    e. assisting the Administrator in developing and maintaining a centralized security data base of all Federal facilities

Adapted from U.S. Government Accountability Office, *Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices* (GAO-05-49) (Washington, DC: U.S. Government Accountability Office, 2004); Exec. Order No. 12977, "Interagency Security Committee," 60 C.F.R. (54411–54412), 54412.

Since the 1995 Oklahoma City bombing, federal facilities and employees continue to be attacked and threatened. For example, in 2010, an anti-IRS extremist flew his single-engine Piper aircraft into an IRS facility in Austin, Texas, destroying the facility and killing one IRS employee.[22] In 2013, a mentally disturbed Department of Defense (DOD) civilian employee killed 12 people at the Washington Navy Yard with a shotgun.[23] Since 2014, the federal government has been warning law enforcement about

[22] Michael Brick, "Man Crashes Plane into Texas IRS Office," *New York Times,* February 19, 2010.

[23] Peter Hermann and Ann E. Marimow, "Navy Yard Shooter Aaron Alexis Driven By Delusions," *Washington Post,* September 25, 2013.

the Islamic State's intentions to kill government employees.[24] These incidents show that the threat to federal facilities and employees is in no danger of dissipating any time soon.

Since the creation of the ISC, federal facility security has remained an important issue for Congress, as evident by the many hearings and requested Congressional Research Service (CRS) and Government Accountability Office (GAO) reports regarding security deficiencies at federal facilities. These reports have consistently found that federal facility security is not adequate. Insufficient contract security guard training, FPS risk assessment methodology, and lack of coordination among federal agencies have been recurring themes throughout these reports. Additionally, the DHS Office of Inspector General (DHS-OIG) has identified deficiencies with how FPS protects federal facilities.[25]

In 2014, the GAO highlighted that federal facilities are vulnerable to cyberattacks through facility BAS networks.[26] The GAO report found that adequate risk assessments were not being conducted, and the DHS had no strategy to secure these networks. Until October 1, 2014, the DHS did not provide adequate guidance for federal agencies to report computer security incidents related to ICS.[27] Additionally, the GAO found that the DHS, through the ISC, had not included cybersecurity threats in the ISC-produced Design-Basis Threat (DBT) report.[28] The DBT outlines the "characteristics of the threat environment to be used in conjunction with all ISC standards."[29] The DHS could leverage lessons learned in federal facility physical security over the last 20 years and apply them to this new cyber risk to federal facilities.

---

[24] "Feds Warn of Possible ISIS-Inspired Attacks on Police, Government Officials, Media," *Fox News*, October 14, 2014, http://www.foxnews.com/politics/2014/10/14/feds-dhs-warn-possible-isis-attacks-on-cops-government-officials-media/.

[25] Office of Inspector General, *Federal Protective Service: Contract Guard Procurement and Oversight Process Challenges* (OIG-09-51) (Washington, DC: U.S. Department of Homeland Security, 2009), https://www.oig.dhs.gov/assets/Mgmt/OIG_09-51_Apr09.pdf.

[26] U.S. Government Accountability Office. *Federal Facility Cybersecurity*, 17.

[27] Ibid.

[28] U.S. Government Accountability Office. *Federal Facility Cybersecurity*, 19.

[29] Ibid.

B. THREATS AND VULNERABILITIES TO BAS/ICS

The networks that comprise the Internet were built for convenience and ease of use, not for security.[30] The 1997 Presidential Commission on Critical Infrastructure Protection claimed, "The day may be coming when an enemy can attack us from a distance, using cyber tools without first confronting our military power and with a good chance of going undetected. The new geography is borderless cyber geography whose major topographical features are technology and change."[31] That day has already come, and attacks against BAS/ICS are constantly occurring.[32] During FY 2014, the United States Computer Emergency Response Team (US-CERT) processed 52,367 cybersecurity incidents for federal agencies.[33] These incidents included denial of service attacks, improper usage, unauthorized access, social engineering, phishing, malicious code installation or execution, and suspicious network activity.[34] While these statistics do not address BAS specifically, they do highlight that federal government networks in general are under constant attack.

The National Institute of Standards and Technology (NIST) uses the term industrial control system (ICS) to generally describe several types of control systems. These control systems include building automation systems (BAS), and many others. Often, BAS technologies are used in critical infrastructure industries to provide for a centralized location to manage remotely or on site to multiple facility systems, such as HVAC, access control, elevators, lighting, security countermeasures, and fire

---

30 Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Santa Barbara, CA: Praeger, 2013).

31 President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, DC: White House, 1997).

32 Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Year in Review 2012* (Washington, DC: U.S. Department of Homeland Security, 2012), https://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2012_Final.pdf.

33 Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act* (Washington, DC: Executive Office of the President, 2015), 14, 16, 17, https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.

34 Ibid., 15.

suppression.[35] Facility BAS were originally implemented as isolated, separate networks; today, however, many of these BAS are accessible to anyone with an Internet connection, thus placing them at risk for exploitation.[36]

Threats to BAS/ICS can come from a variety of sources, including terrorists, criminals, malicious actors, insider threats (disgruntled employees), foreign governments, human error, equipment failure, and natural disasters.[37] There are many reasons for the escalating risk control systems face, including: (1) the move from proprietary software platforms to "the adoption of standardized technologies with known vulnerabilities," such as Microsoft Windows, (2) "the connectivity of control systems to other networks," such as BAS networks integrated within the GSA enterprise network, (3) "constraints on the implementation of existing security technologies and practices," such as poor password management programs, (4) insecure remote connections, such as those that may be in use by the private contractors who maintain the majority of federal facility BAS networks, and (5) "the widespread availability of technical information about control systems" on the Internet.[38]

The GAO found that control systems can be vulnerable to successful cyber-attacks if threat actors execute one or more of the following actions to conduct the attack:

- disrupt the operation of control systems by delaying or blocking the flow of information through control networks, thereby denying availability of the networks to control system operators
- make unauthorized changes to programmed instructions in controllers, change alarm thresholds, or issue unauthorized commands to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as

---

[35] Keith Stouffer, *NIST Briefing: ICS Cybersecurity Guidance—NIST SP 800-82, Guide to ICS Security* (Gaithersburg, MD: National Institute of Standards and Technology, 2013), http://www.businessofsecurity.com/docs/BOS_NIST%20ICS%20Briefing_Keith%20Stouffer%208-28-13.pdf.

[36] Alex Salkever, "If These Networks Get Hacked, Beware," *Business Week*, September 15, 2003, http://www.businessweek.com/stories/2003-09-15/if-these-networks-get-hacked-beware.

[37] Stouffer, *NIST Briefing*.

[38] U.S. Government Accountability Office, *Critical Infrastructure Protection: Challenges in Securing Control Systems* (GAO-04-140T) (Washington, DC: U.S. Government Accountability Office, 2003), 11, http://www.gao.gov/assets/120/110405.pdf.

prematurely shutting down transmission lines), or even disabling of control equipment

- send false information to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators
- modify the control system software, producing unpredictable results
- interfere with the operation of safety systems[39]

Federal facility BAS networks face both unintentional and intentional threats that can be targeted or nontargeted.[40] Unintentional threats to BAS can cause disruptions from software updates or improper maintenance procedures.[41] An intentional threat includes both nontargeted and targeted attacks.[42] A nontargeted attack is achieved when a threat actor releases a worm, malware, or virus with no specific target.[43] A targeted attack occurs when an individual or group attacks a specific system at a specific location.[44] A successful cyber-attack on a federal facility BAS/ICS could result in physical damage if a facility's HVAC system is tampered with, causing server rooms to overheat. Loss of life could also occur if the facility's fire suppression system is disabled. Loss of federal employee productivity could be substantial if the facility is forced to close, and could disrupt government benefits for the nation's veterans and social security recipients.[45]

The FBI remains concerned about the potential threat disgruntled insiders pose to government networks.[46] Often, these insiders have unrestricted access and can steal assets or cause damage without significant knowledge of computer-network intrusion

---

[39] U.S. Government Accountability Office. *Critical Infrastructure Protection*, 14.

[40] U.S. Government Accountability Office, *Multiple Efforts to Secure Control Secure Control Systems Are Under Way, but Challenges Remain* (GAO-07-1036) (Washington, DC: U.S. Government Accountability Office, 2007), 12, http://www.gao.gov/assets/270/268137.pdf.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] Office of Inspector General, *DHS Can Make Improvements to Secure Industrial Control Systems*.

[46] U.S. Government Accountability Office. *Critical Infrastructure Protection*, 7.

techniques.[47] Although there have been no publically disclosed cyber-attacks perpetrated against a federal facility BAS owned by GSA, successful cyber-attacks have already been perpetrated against many other ICS and specifically BAS, and will be discussed in further detail later in this chapter.

In 2012, the Industrial Control System Cyber Emergency Response Team (ICS-CERT) "tracked 171 unique vulnerabilities affecting 55 ICS products."[48] Complicating matters, much information on BAS/ICS design and their locations is publicly available over the Internet.[49] Additionally, "many former employees, vendors, contractors, and other end users of the same ICS equipment worldwide who have inside knowledge about the operation of control systems and their processes."[50] This knowledge could be used to exploit known vulnerabilities within the security of these systems.[51]

Research shows that it is possible for attackers using publicly available information, and with "very little knowledge of control systems to gain unauthorized access to a control system with the use of automated attack and data mining tools and a factory-set default password."[52] It is up to the users to change default passwords, and many never do.[53] Once passwords are reset, the attacker could "lock-out" system operators and alter the control system.[54] Since 2010, ICS-CERT has been warning critical infrastructure operators of the existence of Shodan—a search engine used to discover Internet-facing BAS/ICS systems throughout the world.[55] Once BAS/ICS are discovered

---

[47] U.S. Government Accountability Office. *Critical Infrastructure Protection*, 7.

[48] *ICS-Cert Monitor*, October/November/December 2012: 6, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf

[49] U.S. Government Accountability Office, *Critical Infrastructure Protection*.

[50] Keith Stouffer, Joe Falco, and Karen Scarfone, *Guide to Industrial Control Systems (ICS) Security* (NIST Special Publication 800-82) (Gaithersburg, MD: National Institute of Standards and Technology, 2011), 3–16, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

[51] Stouffer, Falco, and Scarfone, *Guide to ICS Security*.

[52] Ibid.

[53] Stouffer, Falco, and Scarfone, *Guide to ICS Security*, 14.

[54] Ibid., 15

[55] Industrial Control Systems Cyber Emergency Response Team, *Control System Internet Accessibility* (ICS-ALERT-10-301-01) (Washington, DC: U.S. Department of Homeland Security), http://ics-cert.us-cert.gov/alerts/ICS-ALERT-10-301-01.

using Shodan, it is possible for an unauthorized user to access the control system and make changes to the system remotely over the Internet.[56] Although Shodan continues to be an issue, at the urging of the DHS, some of these vulnerabilities in private-sector systems have been eliminated.[57] This threat may be further heighten for federal facilities that house national security agencies due to the cyber capabilities of nation states such as China and Russia.

The GSA's failure to write effective memorandums of agreement (MOA) with the contractors who maintain some federal facility BAS networks has left the government with a complete lack of knowledge about specific vulnerabilities that exist on these networks, or whether trespasses, intrusion attempts, or actual intrusions have occurred. Although general ICS network vulnerabilities are well documented, as are the threats the networks face from adversaries, successful attacks have already been perpetrated against BAS/ICS.

Perhaps the most widely reported attack against a BAS/ICS came in 2010 with the public disclosure of the Stuxnet computer worm. Stuxnet was reportedly used to cause an Iranian uranium enrichment facility to malfunction, delaying Iran's ability to produce uranium, presumably used for the creation of a nuclear weapon.[58] "This sea-change in cyber vulnerability is reminiscent of the transformative changes that attended the explosion of the first atomic bomb."[59] Stuxnet eventually found its way into the networks of critical infrastructure providers from Germany to India and is now publicly available.[60] If a federal facility BAS/ICS became infected by the Stuxnet worm, related disruptions could conceivably affect the federal government's ability to provide essential services to

---

[56] Industrial Control Systems Cyber Emergency Response Team, *Control System Internet Accessibility*.

[57] *ICS-Cert Monitor*, October/November/December 2012.

[58] Michael B. Kelly, "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," *Business Insider*, November 20, 2012, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

[59] Rosenzweig, *Cyber Warfare*, 2, 7.

[60] Dennis Fisher and Paul Roberts, "Threat Post: Stuxnet," Kaspersky Lab, accessed October 21, 2015, http://usa.kaspersky.com/sites/usa.kaspersky.com/files/TP-Spotlight-Stuxnet.pdf.

citizens dependent on agencies such as the Social Security Administration and Department of Veterans Affairs for a considerable amount of time.[61]

While it is difficult to argue the inconveniences federal employees and visitors to federal facilities could experience resulting from a disruption to a BAS—such as elevator failure, fire suppression system activations, and temperature fluctuations—there are potentially life-threatening consequences as well. "In March 1997, a teenager in Worcester, Massachusetts used a dial-up modem" connected to a public-switched telephone network to disable the telephone network system.[62] His actions rendered phone service inoperable at several Worcester airport facilities, including "the control tower, airport security, the airport fire department, the weather service" and all airlines located at the airport.[63] Additionally, "the tower's main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress."[64] The attack shut down telephone service for businesses and approximately 600 homes in a nearby town.[65]

In January 2012, using open-source information, ICS-CERT identified and responded to a cyber-intrusion affecting the heating and air conditioning at an unnamed GFS facility.[66] The facility's personnel reported they discovered unauthorized changes had been made to the Energy Management System control settings, resulting in warmer than normal temperatures inside the facility.[67] As a result of the discovery, facility personnel reset the system settings to normal values and assured the BAS/ICS was no

---

[61] Paul Kerr, John Rollins, and Catherine Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (CRS Report R41524) (Washington, DC: Congressional Research Service, 2010), http://assets.opencrs.com/rpts/R41524_20101209.pdf.

[62] Pierre Thomas, "Teen Hacker Faces Federal Charges," *CNN*, March 18, 1998, http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html .

[63] Ibid.

[64] Ibid.

[65] Ibid.

[66] "Government Facilities Sector," *ICS-CERT Monthly Monitor*, (February 2012): 1, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Feb2012.pdf.

[67] Ibid.

longer accessible via the Internet.[68] ICS-CERT determined an unauthorized user had changed the temperature via the Internet, despite the BAS/ICS requiring a password for remote login.[69] ICS-CERT informed the author the attack occurred at a law enforcement crime lab. It is unknown if any evidence was compromised as a result of the attack; however, it is clear the potential was there. On the surface, these actions appear only to affect general comfort. Further analysis, however, indicates a potential for a significant loss of productivity, if employees were sent home until the problem was resolved.

In 2012, a cybersecurity company initiated a mock ICS that mimicked a water-pump network connected to the Internet to determine vulnerabilities within the network.[70] The existence of the ICS water-pump station was quickly discovered by hackers, who began to tamper with the system.[71] Researchers from the cybersecurity company began collecting data to determine how often and from where targeted attacks originated. Analysis indicated 12 attempts to shut down the water pump and five attempts to modify the pump's processes were made from multiple countries; approximately 33 percent of the attacks originated in China, followed by 19 percent in the United States.[72] The remaining attacks were carried out by people in Russia, Laos, and the Palestinian territories.[73] President Obama's *International Strategy for Cyberspace*, released in 2011, broadly indicates the national security and diplomatic implications of confirmed state-sponsored cyber-attack against the United States could be significant, potentially leading to economic and or diplomatic ramifications for the country that carried out the attack.[74]

---

68 "Government Facilities Sector," *ICS-CERT Monthly Monitor*, (February 2012).

69 Ibid.

70 John Leyden, "SCADA Honeypots Attract Swarm of International Hackers," *The Register*, March 20, 2013, http://www.theregister.co.uk/2013/03/20/scada_honeypot_research/.

71 Ibid.

72 Ibid.

73 Leyden, "SCADA Honeypots."

74 President of the United States, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: White House, 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

C. RESEARCH QUESTIONS

This thesis examines current legislation and DHS cyber capabilities, and answers the following primary research question:

- How can the DHS leverage existing federal laws, presidential directives, executive orders, frameworks, and its current cyber and investigative capabilities to establish a strategy to secure federal facility building-automation system networks?

The following secondary research questions are answered to properly address the primary research question:

- If existing resources are not sufficient, what additional resources should be obtained to mitigate the risks?
- How should the DHS leverage its components' law enforcement authorities to augment technical cyber defense measures?

D. METHODOLOGY

By analyzing policy options, this thesis examines legislation, executive orders, presidential directives, and government frameworks to determine if the DHS more broadly, has the legal authority to secure federal facility BAS. Analysis of specific DHS components such as the USSS and the NPPD and its subcomponents—ICS-CERT, FPS, and NCCIC—was conducted to determine if the DHS can secure federal facility BAS with existing resources or if additional resources are required.

There are well over 200,000 federal facilities around the world currently employing building-automation system technology, some owned and some leased. This thesis only addresses non-DOD federal facilities owned by the GSA. This limitation reduces the number of facilities affected by this inquiry from over 200,000 to approximately 1,500. This thesis does not attempt to prove the networks that control building automation systems are vulnerable; it is widely accepted by cybersecurity experts that if a network is connected to the Internet, then the network is vulnerable to cyber-attacks.[75] Additionally, because no entity is assessing the security of these specific

[75] "The Importance of Cyber Hygiene in Cyberspace," INFOSEC Institute, April 30, 2015, http://resources.infosecinstitute.com/the-importance-of-cyber-hygiene-in-cyberspace/.

networks, it is impossible to provide evidence proving or disproving whether they are secure or not.

Sources for this project include government and academic data. Presidential directives, executive orders, legislation, government frameworks, regulatory publications, specific government agency information, and scholarly journals and books related to the thesis topic were used to support the research. No surveys or interviews were included in the research. At the conclusion of this thesis, DHS leadership will have a clearer understanding of the vulnerabilities to federal facility building automation systems, as well as more in-depth knowledge of the Department's authority and resources to pursue a strategy to secure them.

E. CHAPTER OVERVIEW

Chapter II provides a literature review summarizing existing knowledge of the topic. The review includes sources from the private sector, government, and academia to enhance understanding of current authorities to execute cybersecurity function by the Department of Homeland Security.

Chapter III evaluates the current status of federal facility BAS network security. Despite clear legal authorities, a ready-made framework, and congressional pressure to develop a strategy to secure these networks, roadblocks exist. Maintaining the status quo means federal facilities remain vulnerable and the potential consequences could be devastating.

Chapter IV explores how existing DHS capabilities can be leveraged to secure BAS networks. By using the DHS' own continuous monitoring and assessment software, and information sharing platforms, the DHS is well suited for this mission.

Chapter V suggests creating a cyber-program within the FPS to incorporate risk assessments of BAS networks within their presidentially mandated Facility Security Assessments. Additionally, developing a capability to conduct criminal investigations into BAS network intrusions is evaluated.

Chapter VI examines a hybrid approach to securing federal facility BAS through combining existing resources such as software, incident response frameworks, and investigative authority, in collaboration with private sector expertise.

Chapter VII provides comparative analysis of the options offered in Chapters IV, V, and VI, and each is judged by the following categories: DHS acceptability, compliance (laws, E.O.s, presidential directives), effectiveness, implementation, institutional acceptability, and time to implement the preferred option.[76] This chapter identifies the preferred option as initially using cybersecurity contractors to perform network risk assessments and USSS personnel to conduct criminal investigations into cyber intrusions until the FPS can establish an effective program.

[76] Consolini, "Regional Security Assessments."

II. LITERATURE REVIEW

The purpose of this literature review is to summarize the existing knowledge of cybersecurity issues for Industrial Control Systems (ICS) inside federal facilities, and more specifically of Building Automation Systems (BAS), which is a subset of ICS. Subsequently, the literature evaluated is heavily focused on the more generic term, ICS, and the general issues with securing them (which can also be applied to BAS in most instances). The sources reviewed come from federal government investigative reports, legislation, executive orders and presidential directives, federal government frameworks to secure ICS, and scholarly journals and books.

Historically, the Department of Homeland Security (DHS) has focused its efforts on protecting private sector Industrial Control Systems (ICS), not BAS that run federal facility processes like HVAC, lighting, and elevators. "From fiscal year 2011 to fiscal year 2014, the number of cyber incidents reported to the DHS involving industrial control systems, which include building and access control systems, increased from 140 incidents to 243 incidents, an increase of 74 percent."[77] This increase in incidents highlights the need for DHS to develop an executable strategy in the near term.

A. FEDERAL GOVERNMENT REPORTS

For over 17 years, the U.S. government has been concerned with cyber-attacks against critical infrastructure.[78] A 1997 presidential commission on critical infrastructure (CI) protection recognized the role of the cyber realm in CI.[79] Though no evidence was found of an impending cyberattack on CI, the commission did not rule out that vulnerabilities existed, and in their findings said "that vulnerability jeopardizes our national security, global economic competitiveness, and domestic wellbeing."[80] The commission made several recommendations to improve CI cybersecurity, to include

[77] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 14.

[78] Presidential Commission on Critical Infrastructure Protection, *Critical Foundations*.

[79] Ibid.

[80] Ibid., Forward vii.

developing a national cyber threat warning capability, creating information-sharing relationships with the private sector, recruiting cybersecurity personnel, and creating legislation to address cybersecurity issues.[81] Seventeen years later, the federal government is still struggling to implement many of the 1997 committee's recommendations.

Because the threat itself is still evolving, so is the literature on this topic; there is a split among experts on the potential consequences of a cyber-attack on CI. Early on, the U.S. intelligence community could not reach a consensus on the imminence and scale of what, at the time, was an unsubstantiated threat.[82] Others believe a successful attack would have a significant impact, but it would be unlikely that an attack could succeed.[83] Almost all of the government documents reviewed that address ICS cybersecurity acknowledge the federal government owns facilities that operate ICS. However, these references are mostly limited to ICS that run oil, water, gas, energy, and nuclear facilities, not federal facilities that house such agencies as the Department of Veterans Affairs and the Social Security Administration.

When ICS were originally designed, they were not intended to be connected to the Internet. As a result, older systems have been retrofitted to ensure network access, creating connections that are not optimal for cybersecurity.[84] In the early days of ICS cybersecurity initiatives, experts were split on the possibility of a catastrophic cyber-attack on an ICS and the potential consequences. The general consensus was that successful cyber-attack would not likely result in casualties, but infrastructure service could be disrupted while attempts were being made to regain control of the system from the hacker and any damage repaired.[85] Experts placed even less probability of cascading effects of ICS failure, such as a cyber-attack causing other infrastructures to fail. When

---

[81] Presidential Commission on Critical Infrastructure Protection, *Critical Foundations*, Forward vii.

[82] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post*, June 27, 2002, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html.

[83] Dana A. Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat* (CRS Report RL31534) (Washington, DC: Congressional Research Service, 2003).

[84] Ibid.

[85] Ibid.

viewed through the lens of federal facility BAS, the potential for a catastrophic effect is immense—a cyber-attack could disrupt network servers that run individual agencies, causing them to overheat, and rendering them inoperable. In 2014, the Social Security Administration estimated they would pay approximately 59 million Americans almost $863 billon in benefits.[86] If these Americans were unable to receive their benefits, prohibiting them from purchasing such necessities as medication, people could die.

In October 2002, the Government Accountability Office (GAO) cited the federal government's responsibility to protect federal facilities, and specifically mentioned critical cyber-based systems located in those facilities.[87] However, the GAO only provided physical security recommendations; no cybersecurity recommendations were made.[88] As far back as 2003, the federal government was touting cybersecurity programs for ICS in federal facilities, implemented by the Department of Energy (DOE), Department of Defense (DOD), and the National Institute for Standards and Technology (NIST). It was not until 2014, however, that the GAO would release a report addressing this issue specifically for GSA-owned federal facilities.[89]

By 2007, Congress became so concerned with cyber threats to ICS, they tasked the GAO to determine specific existing threats and vulnerabilities. The GAO was also tasked with understanding potential consequences of a cyber-attack, as well as identifying challenges to secure these systems, by determining if best practices from the private sector could be leveraged, and whether or not the private sector was effective in its efforts.[90] The 2007 GAO report suggested that, in addition to the technical roadblocks, there were organizational roadblocks in securing ICS, including "difficulty in developing

---

[86] "Social Security Basic Facts," Social Security Administration, April 2, 2014, www.ssa.gov/news/press/basicfacts.html.

[87] U.S. Government Accountability Office, *Building Security: Security Responsibilities for Federally Owned and Leased Facilities* (GAO-03-8) (Washington, DC: U.S. Government Accountability Office, 2002), 14.

[88] Ibid.

[89] Shea, *Critical Infrastructure*; U.S. Government Accountability Office. *Federal Facility Cybersecurity*, 22.

[90] U.S. Government Accountability Office, *Multiple Efforts to Secure Control Secure Control Systems*, 32.

a compelling business case for improving ICS security, a reluctance to share information on ICS incidents and division of technical responsibilities within an organization." The report continued, "Until industry users of control systems have a business case to justify why additional security is needed, there may be little market incentive for the private sector to develop and implement more secure control systems."[91] Although the GAO was specifically referencing the challenges for the private sector, these challenges are just as relevant for the federal government.

In 2009, the DHS Office of Inspector General (OIG) addressed the DHS's progress in securing ICS in the private sector and failed to mention that these systems are found within federal facilities. This report, like others, improve situational awareness of the issue by focusing on improving cybersecurity information-sharing with the private sector, conducting vulnerability assessments, measuring effectiveness of private sector ICS cybersecurity programs, and suggesting formal training.[92]

A 2014 GAO report on the cyber risks to federal facility BAS found the DHS and GSA are not in compliance with the Federal Information Security Management Act (FISMA), which requires the completion of federal facility BAS risk assessments, among other failures.[93] Additionally, the DHS was found to have no strategy to address risks to BAS, because threats to these systems are "an emerging issue."[94] Prior to October 2014, the DHS did not include ICS on the list of systems for which federal agencies were required to report computer security incident occurrences, reducing the number of reported incidents to one.[95] The report found that a cyber-attack on a BAS could affect a federal agency's organizational operations, individuals, assets, reputation, and image.[96] The report identified criminal groups, corrupt employees, hackers, and terrorists as

---

[91] U.S. Government Accountability Office, *Multiple Efforts to Secure Control Secure Control Systems,* 20.

[92] Office of Inspector General, *Challenges Remain in DHS' Efforts to Secure Control Systems*, (OIG-09-95), Washington, DC: U.S. Department of Homeland Security, 2009), https://www.oig.dhs.gov/assets/Mgmt/OIG_09-95_Aug09.pdf.

[93] U.S. Government Accountability Office, *Federal Facility Cybersecurity*.

[94] Ibid., 17.

[95] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 18.

[96] Ibid., 14.

potential threat actors that could disrupt a federal facility BAS. The capabilities and intentions of threat actors was found to vary from political or monetary motivations to mischief.[97]

The GAO recommended that the DHS develop a strategy in cooperation with the GSA that:

- defines the problem
- identifies the roles and responsibilities
- analyzes the resources needed
- identifies a methodology for assessing cyber risk to building and access control systems.[98]

B. LEGISLATION

The second set of literature on this topic consists of cybersecurity legislation passed by Congress and signed into law by the president. To answer the research question, it is imperative to know what laws exist (and to interpret them accurately) in order to determine if new or amended legislation is required to secure federal facility BAS networks..

Since the days of the Regan Administration, Congress has been concerned about computer security threats; until recently, however, legislation had not kept pace with the proliferation of these threats.[99] During the last two decades, more than 50 cybersecurity-related statutes have been enacted, although none of the statutes specifically address BAS.[100] When FISMA was passed in 2002, it was Congress' first major cybersecurity legislation affecting critical infrastructure; it was subsequently amended in 2014.[101] Approximately one month prior to FISMA's enactment in 2002, President Bush signed the Homeland Security Act of 2002 into law.

---

[97] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 14.

[98] Ibid., 16.

[99] *An Act to Establish the Department of Homeland Security, and for Other Purposes (Homeland Security Act) Act of 2002*, Pub. L. No. 107-296 (2002), Title II Sec. 201 D, 5.

[100] Ibid., 20.

[101] Ibid., 44.

The Department of Homeland Security was established as a result of the Homeland Security Act of 2002. One of the Act's requirements was transferring the Federal Protective Service—which provides security to federal facilities—from GSA to the DHS.[102] The Act also required the DHS to develop a comprehensive plan for securing U.S. critical infrastructure and the "physical and technological assets that support such systems."[103] It also required "DHS to conduct risk assessments of critical infrastructure to determine the risks associated with various types of terrorists attacks and the feasibility of counter measures."[104] Housed within the Homeland Security Act of 2002 is the Cybersecurity Enhancement Act of 2002 (CEA). The CEA increased penalties under the Computer Fraud and Abuse Act, Title 18 Section 1030, for individuals whose "violation was intended to or had the effect of significantly interfering with or disrupting critical infrastructure; and whether the violation was intended to or had the effect of created a threat to public health or safety, or injury to any person."[105]

FISMA provided federal government agency heads with a comprehensive framework to assess risk to their information technology systems. It also required federal agencies to coordinate with the private sector and national security and law enforcement entities, designating NIST as the government agency responsible for developing cybersecurity standards for the federal government. Further, the Act required agency heads to create security controls to mitigate identified risks and periodically test them to ensure they were working effectively. Agency heads must report annually "on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements" to the Director of the Office of Management and Budget (OMB), who must then notify Congress.[106]

---

[102] *An Act to Establish the Department of Homeland Security, and for Other Purposes (Homeland Security Act) Act of 200.*, Stat. 2136 Sec. 403.

[103] Ibid., Sec. 201, D, 5

[104] Ibid, 2.

[105] Ibid., Sec. 225, 2, B, 7, 8.

[106] *E-Government Act of 2002 (FISMA of 2002)* Pub. L. No. 107-347 (2002), 116.

Recent congressional cybersecurity legislative proposals have mostly focused on matters in 10 broad areas. These areas have been defined as:

- national strategy and the role of government
- FISMA reform
- protection of critical infrastructure
- information sharing and cross-sector coordination
- breaches resulting in the theft or exposure of personal data such as financial information
- cybercrime
- privacy in the context of electronic commerce
- international efforts
- research and development
- cybersecurity workforce[107]

In 2014, FISMA was amended to provide the secretary of the DHS the authority to implement "binding operational directives" to federal government agencies.[108] FISMA's 2014 revision is wide ranging; however, only the provisions affecting this inquiry were included. 2014 FISMA defines "binding operational directives" as "compulsory direction for the purpose of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability or risk."[109] Additionally, the Act modified federal agency reporting requirements to ensure federal agencies report specific information about cybersecurity incidents and threats. The amendment also requires the director of OMB to report cyber breaches to Congress within 30 days of discovery, to include "the estimated number of

[107] Eric A. Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions* (CRS Report No. R42114) (Washington, DC: Congressional Research Service), 5, https://www.fas.org/sgp/crs/natsec/R42114.pdf.

[108] *Federal Information Security Modernization Act of 2014*, Pub. L. No. 113-283, Stat. 3073 (2014), https://www.congress.gov/bill/113th-congress/senate-bill/2521/text.

[109] *Federal Information Security Modernization Act of 2014 (FISMA of 2014)*, Pub. L. No. 113-283 (2014), 128.

individuals affected, the assessed risk of harm to those individuals, and when notice will be made to those individuals."[110]

In December 2014, President Obama signed into law the National Cybersecurity Protection Act (NCPA) of 2014. The Act amends the Homeland Security Act of 2002 to codify into law the already existing National Cybersecurity and Communications Integration Center located in the DHS to "carry out responsibilities of the DHS Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and related DHS programs."[111] The Center shares real-time information on cybersecurity analysis, risks, incidents, and warnings for both the federal government and private sector across federal and nonfederal platforms.[112] The Act also requires DHS, among other things, to "develop, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks to critical infrastructure."[113] This law makes it possible for DHS to compare malicious code signatures found in private sector ICS and subsequently search for these signatures inside federal facility BAS networks. Knowledge of this information also allows the DHS to block these codes from ever entering DHS-protected networks.

The Cybersecurity Workforce Assessment Act was signed into law on December 18, 2014. The Act requires the DHS secretary to assess the status of cybersecurity professionals within the DHS—specifically, if the workforce is capable of meeting its cybersecurity mission, information on the locations of cybersecurity positions within the department, employee training, and which positions are performed by full-time Department employees, other government agencies, or contractors.[114] The Act further requires the secretary of the DHS to develop a "comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment, and retention of the cybersecurity

---

[110] *Federal Information Security Modernization Act of 2014 (FISMA of 2014)*, 128..

[111] *National Cybersecurity Protection Act of 2014 (NCPA of 2014)*, Pub. L. No. 113-282 (2014), 128.

[112] Ibid.

[113] Ibid., Sec. 7.

[114] *Cybersecurity Workforce Assessment Act (CWAA of 2014)*, Pub. L. No. 113-246 (2014), 128.

workforce of the Department."[115] Under the law, the secretary is required to identify obstacles impeding hiring and future development of the workforce, as well as knowledge gaps within the existing cybersecurity workforce employed by the Department, and a plan to overcome identified gaps.[116]

From the review of available sources, it is clear the biggest disagreement regarding cybersecurity legislation is related to information sharing. Over the last several years, there has been a never-ending stream of executive orders and draft legislation attempting to improve information sharing between the government and the private sector. With the private sector owning and operating over 90 percent of critical infrastructure, information sharing is extremely important to both entities.[117] Major opposition to the legislation is suspected to be related to privacy concerns, most likely intensified in the aftermath of Edward Snowden's disclosures of National Security Agency (NSA) activity. Many private sector companies are concerned that information on their networks' cyber breaches would become public, thus causing company stock prices to fall.[118] Another area of concern is that some of the legislation allows for direct information sharing with the U.S. military by way of NSA.[119]

C. EXECUTIVE ORDERS AND PRESIDENTIAL DIRECTIVES

Presidential executive orders (E.O) and directives related to cybersecurity of critical infrastructure issued by the President George W. Bush and Barack H. Obama Administrations contain the third set of literature that may offer a solution to the research question. Due to the evolution of these orders and directives, only those orders or directives still in effect were analyzed.

---

[115] *Cybersecurity Workforce Assessment Act (CWAA of 2014)*, 128.

[116] Ibid.

[117] David H. McElreath et al., *Introduction to Homeland Security*, 2nd Edition (Boca Raton, FL: CRC Press, 2013), 114.

[118] N. Eric Weiss, *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis* (CRS Report No. R43821) (Washington, DC: Congressional Research Service, 2015).

[119] *Cybersecurity Information Sharing Act of 2015*, S.754, 114th Cong., 1st sess. (2015).

Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, was signed on October 16, 2001. This E.O. established a protection program "to secure information systems for critical infrastructure" and specifically mentioned "protection of federal departments and agencies' critical infrastructure," and "the physical assets that support such systems."[120] The E.O. called for a voluntary public-private partnership and held executive department agency heads responsible for their agencies' information systems' security. Cyber threat information sharing was also included in the Order to manage "threat warning, analysis, and recovery of information among government network operation centers."[121] E.O. 13231 requires cyber incident coordination and response, support for law enforcement investigations into cyber incidents, and research and development, as well as provisions for the federal cybersecurity workforce.[122]

In February 2013, Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (PPD-21), was released.[123] The Directive supersedes HSPD-7, and established a national policy on CI security and resilience, and identifies the secretary of the DHS as the lead federal coordinator. The Directive makes clear the responsibility to secure CI is shared among federal, state, and local entities, to include private and public CI operators and owners.[124] The Directive identifies three strategic imperatives that will drive the federal government's approach to "strengthen critical infrastructure security and resilience":

1. Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience
2. Enable effective information exchange by identifying baseline data and systems requirements for the federal government

---

[120] Exec. Order No. 13231, *Critical Infrastructure Protection in the Information Age* (2001), Sec. 1.

[121] Ibid., Sec. 5.

[122] Ibid.

[123] President of the United States, *Presidential Policy Directive—Critical Infrastructure Security and Resilience* (PPD-21) (Washington, DC: White House, 2013).

[124] President of the United States, *Presidential Policy Directive—Critical Infrastructure Security and Resilience.*

3. Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure[125]

Further, the Directive ensures "all federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions."[126] The FBI is identified as the lead investigative agency for attempted attacks, actual attacks, or sabotage perpetrated against critical infrastructure emanating from overseas.[127] However, the Directive does not identify what federal investigative entity is responsible for cyber-attacks against critical infrastructure perpetrated from inside the United States. The FBI is also named as the agency to lead the National Cyber Investigative Joint Task Force (NCIJTF), which includes DHS representation. The Directive requires the GSA, in consultation with DHS, to "provide or support government-wide contracts with critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure."[128]

In February 2015, the Interagency Security Committee (ISC) released a white paper to address the implementation of PPD-21. The ISC was created in 1995 when President Clinton signed E.O. 12977 to strengthen federal facility security in the wake of the Oklahoma City bombing in 1995.[129] The ISC established a working group consisting of the DHS, GSA, and other federal agencies to "address cyber threats in relation to physical security measures at federal facilities."[130] The working group decided the ISC must include cyber threats to BAS in the ISC-produced Design Basis Threat Report (DBT), and develop countermeasures for them. This is likely due to the recommendations GAO made to the DHS secretary in December 2014.[131] The DBT outlines the 31

[125] President of the United States, *Presidential Policy Directive—Critical Infrastructure Security and Resilience*.

[126] Ibid.

[127] Ibid.

[128] Ibid.

[129] Exec. Order No.12977, *Critical Infrastructure Protection in the Information Age* (1995–2001), Sec. 5 (a) (2).

[130] President of the United States, *Presidential Policy Directive—Critical Infrastructure*, 1.

[131] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 24.

undesirable events most likely to occur at a nonmilitary federal facility. Finally, the ISC recommended the ISC Training Subcommittee seek to advise ISC members to identify training programs to ensure compliance with PPD-21.[132]

On January 9, 2008, a classified National Security Presidential Directive (NSPD) /Homeland Security Presidential Directive (HSPD) (known as NSPD-54/HSPD-23 was issued and subsequently declassified on June 5, 2014.[133] The Directive requires all federal agencies to "provide DHS with visibility and insight into the status of their federal systems and shall respond to DHS direction in areas related to network security."[134] However, the Directive makes it clear that federal agencies are still responsible to defend and protect their own computer networks. The DHS intrusion detection program, EINSTEIN, was directed to be deployed to all federal systems to enhance security for those systems.[135] HSPD-23 also requires the DHS secretary and the attorney general to ensure they make adequate support available for those DHS and Department of Justice employees charged with deterring, disrupting, and defending against illegal computer activity domestically, to include the application of law enforcement capabilities.[136]

D. GOVERNMENT FRAMEWORKS

Several cybersecurity frameworks exist around the world relating to securing ICS; however, the fourth set of literature focuses on only two: one from the DHS and the other from the NIST. This is to ensure this inquiry remains consistent with existing legislation and E.O.s. In 2006, federal agencies established a working group to discuss issues with

---

[132] Interagency Security Committee, *Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper* (PPD-21) (Washington, DC: Department of Homeland Security), http://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf.

[133] National Security Council, *Cybersecurity Policy* (NSPD-54/HSPD-23) (Washington, DC: White House, 2008). https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf.

[134] Ibid.

[135] Ibid.

[136] National Security Council, *Cybersecurity Policy* (NSPD-54/HSPD-23) (Washington, DC: White House, 2008). https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf.

securing control systems.[137] The working group tasked its members with providing information on how and why they use control systems and in what ways they coordinate with other agencies. Twenty-eight federal agencies submitted data, including 12 sector-specific agencies as outlined by the National Infrastructure Protection Plan (NIPP).[138] The Department, as the lead federal entity, was tasked with guiding "a cohesive effort between government and industry."[139] The working group reported that the Government Facilities Sector (GFS) shared their control system efforts; there is no indication, however, that GSA was present, as their efforts to incorporate a network capability into their BAS had not yet begun.[140]

In 2009, the DHS National Cyber Security Division developed the *Strategy for Securing Control Systems* as part of the Department's responsibility to lead and coordinate efforts to increase control system security for the nation's critical infrastructure.[141] The *Strategy* was developed in response to a 2007 GAO report (cited previously) that outlined deficiencies in ICS security.[142] The *Strategy* created the Industrial Control Systems Joint Working Group and expanded the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which is tasked with responding to cyber incidents affecting public and private sector CI.[143] The *Strategy* relies on the risk management framework contained within the NIPP and offers guidance on coordination, research and development, roles and responsibilities, incident response, information sharing, best practices, and regulation.[144] Ironically, the Commercial Facilities Sector (CFS), which also employs BAS to control their HVAC, security

---

[137] President of the United States, *Presidential Policy Directive—Critical Infrastructure Security and Resilience.*

[138] Ibid.

[139] Ibid.

[140] Ibid.

[141] U.S. Department of Homeland Security, *Strategy for Securing Control Systems: Coordinating and Guiding Federal, State, and Private Sector Initiatives* (Washington, DC: U.S. Department of Homeland Security, 2009), https://ics-cert.us-cert.gov/sites/default/files/documents/Strategy%20for%20Securing%20Control%20Systems.pdf.

[142] U.S. Department of Homeland Security, *Strategy for Securing Control Systems*, 1.

[143] U.S. Department of Homeland Security, *Strategy for Securing Control Systems*, 2.

[144] U.S. Department of Homeland Security, *Strategy for Securing Control Systems*, 4.

systems, and telecommunications functions, is cited in the *Strategy* for control system security efforts, but federal facility BAS is not.[145] Approximately 8,000 GSA-leased facilities are located in CFS facilities.[146]

In June 2011, NIST released Special Publication 800–82, *Guide to Industrial Control Systems (ICS) Security*. The NIST guide was updated in 2013 and again in May 2015, and is recognized as the essential framework to enhance cybersecurity of ICS, including BAS for the private and public sectors but excluding national security systems.[147] Included within the NIST framework are typical threats and vulnerabilities associated with ICS, countermeasures to mitigate them, and risk management practices.[148]

The NIST has identified three all-embracing types of control system incidents:

- Intentional targeted attacks such as gaining unauthorized access to files, performing a DoS, or spoofing emails (i.e., forging the sender's identity for an email)
- Unintentional consequences or collateral damage from worms, viruses or control system failures
- Unintentional internal security consequences, such as inappropriate testing of operational systems or unauthorized system configuration changes[149]

Although potentially the most consequential, NIST research found that targeted attacks are the least likely to occur and also require "detailed knowledge of the system and supporting infrastructure."[150] NIST determined the most likely threats to control systems originate from "disgruntled employees, former employees and others who have worked for the organization."[151]

---

[145] U.S. Department of Homeland Security, *Strategy for Securing Control Systems*, 38.

[146] General Services Administration, "Inventory of Owned and Leased Properties," accessed June 13, 2015, http://www.gsa.gov/portal/content/100783.

[147] Stouffer et al., *Guide to ICS Security*.

[148] Ibid.

[149] Stouffer et al., *Guide to ICS Security*.

[150] Ibid.

[151] Ibid.

E. SCHOLARLY JOURNALS AND BOOKS

ICS have evolved since they first appeared as stand-alone systems in the 1950s.[152] Today, ICS are used to "remotely monitor and control the delivery of essential services and products" such as water, electricity, and gas.[153] Originally, security was not considered because they were designed as closed systems, not accessible by the Internet. The literature differs regarding the capabilities required to carry out a successful attack against an ICS. Some schools of thought believe a high level of knowledge of ICS is needed, while others believe attackers could randomly stumble onto an ICS network while attempting to target something else.[154] The difference in opinion seems to be tied to the rapidly evolving nature of available information on ICS posted to the Internet by hackers. Several risk frameworks have been published by both government and industry and they remain remarkable similar; some schools of thought, however, consider the likelihood of an ICS cybersecurity incident by reviewing past records, published literature, experiments, and market research of vendors.[155]

The integration of ICS with other corporate systems (much like GSA has done) means information from the BAS/ICS could be fed directly into the corporate system.[156] This was the approach hackers took in 2013 with the Target department store breach, as noted by Jaikumar Vijayan of *Computer World* magazine. Hackers stole login credentials

---

[152] "News of Science," *American Association for the Advancement of Science* 122, No. 3169 (September 1955), 555.

[153] Christopher Begg and Matthew Warren, "Safeguarding Australia from Cyber-terrorism: A SCADA Risk Framework," in *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions*, ed. John Walp, Manish Gupta, and Raj Sharman: 369–84, (Hershey, PA: IGI Global, 2012), doi: 10.4018/978-1-4666-0197-0.ch021.

[154] Tyson Macaulay and Bryan Singer, *Cybersecurity for Industrial Control Systems* (Boca Raton, FL: CRC Press, 2012), 59.

[155] Macaulay and Singer, *Cybersecurity for Industrial Control Systems*, 373.

[156] Antony Bridges, "Industrial Control Systems; The Human Threat," in *Securing Critical Infrastructures and Critical Control Systems Approaches for Threat Protection*, ed. Christopher Lanig, Atta Badii, and Paul Vickers: 82–104, (Hershey, PA: IGI Global, 2013), doi: 10.4018/978-1-4666-2659-1.ch004.

from a third-party vendor responsible for monitoring Target's BAS and remotely entered their network, stealing millions of Americans' credit card information.[157]

BAS are designed to be efficient, safe, productive, and to reduce cost.[158] Ironically, due to a lack of security of federal facility BAS, maintaining those three core goals is in jeopardy. The literature is fairly consistent regarding the vulnerabilities facing BAS. These vulnerabilities are diverse but generic, such as lack of awareness relating to threats and system vulnerabilities, insufficient physical security of ICS, and "insertion of foreign devices."[159] According to Dr. David Brooks, a distinguished network security researcher, many BAS are designed, installed, and operated by service engineers, with little consideration for security.[160] This is also the case for BAS in the majority of GSA-owned facilities.[161] These facilities' BAS networks are not protected behind the GSA firewall, leaving them at risk.[162] However, there are also generic mitigation strategies that can be employed to reduce the risks, such as removing BAS default usernames and passwords. To achieve integration within networks, BAS use open-data communications hardware and protocols, leaving the facilities using the technology vulnerable to both internal and external risks and threats.[163] From a cybersecurity solutions perspective, BAS security is still in its infancy, as they are a relatively new technology.

Another area of agreement among the government literature is the human factor. No matter how robust information security policies are, if employees do not follow them,

---

[157] Jaikumar Vijayan, "Target Attack Shows Danger of Remotely Accessible HVAC Systems," Computer World, February 7, 2014, http://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html.

[158] David Brooks, "Security Threats and Risks of Intelligent Building Systems: Protecting Facilities From Current and Emerging Vulnerabilities," in *Securing Critical Infrastructures and Critical Control Systems Approaches for Threat Protection*, ed. Christopher Lanig, Atta Badii, and Paul Vickers: 1–16, (Hershey, PA: IGI Global, 2013), doi: 10.4018/978-1-4666-2659-1.ch001.

[159] Ibid.

[160] Ibid.

[161] Josh Mordin and Sandy Schadchehr, "Building Monitoring and Control Systems in GSA," presented at the Cybersecurity Building Control Systems Workshop, Washington, DC, March 24, 2015.

[162] Ibid.

[163] Brooks, "Security Threats and Risks," 2.

they are worthless.[164] Humans working within any framework that places a burden on them will seek ways to make their lives easier.[165]

F. CONCLUSION

The existing research into cybersecurity of ICS has generally focused on three key areas: legislation and E.O.s, threats and vulnerabilities, and frameworks to establish an effective cybersecurity program for ICS. The literature review provides a legal foundation to establish a BAS cybersecurity program for federal facilities, backed by E.O.s. Existing DHS and NIST frameworks provide the DHS, and to an extent GSA, a roadmap to begin the tough work of securing these systems.

[164] Bridges, "Industrial Control Systems," 11.

[165] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CURRENT FEDERAL FACILITY BAS NETWORK SECURITY

The current DHS strategy to secure federal facility BAS is nonexistent; recently, however, both the DHS and GSA have agreed to work together to develop one.[166] There are many challenges associated with increasing cybersecurity within the federal government, and specifically cybersecurity of federal facility BAS networks. For example, determining if existing laws are sufficient to prosecute bad actors, finding the balance between security and privacy, determining roles and responsibilities for government agencies, addressing lack of trained personnel, and accounting for the constantly changing nature of the threat have all contributed to these challenges. This chapter analyzes the current roadblocks to achieving security of BAS networks inside federal facilities, cybersecurity law and legal authorities the federal government already possesses to secure federal facility BAS networks, as well as the responsibilities of DHS and GSA in this effort.

A. ROADBLOCKS TO SECURING FEDERAL FACILITY BAS

A 2007 GAO report suggested that, in addition to the technical roadblocks, there are organizational roadblocks in securing ICS, including "difficulty in developing a compelling business case for improving ICS security, a reluctance to share information on ICS incidents and division of technical responsibilities within an organization."[167] The report continued, "Until industry users of control systems have a business case to justify why additional security is needed, there may be little market incentive for the private sector to develop and implement more secure control systems."[168] Although the 2007 GAO report was specifically referencing the challenges for the private sector, the 2014

[166] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, Appendix III, IV.

[167] U.S. Government Accountability Office, *Multiple Efforts to Secure Control Secure Control Systems*. 2, http://www.gao.gov/assets/270/268137.pdf.

[168] Ibid.

GAO report on cyber risks to federal facility BAS identified the same challenges for the federal government.[169]

The difference between traditional information technology (IT) (ensuring the corporate network remains functioning by processing transactions and providing information) and operational technology (OT), (responsible for monitoring and controlling BAS) also presents roadblocks to securing BAS networks.[170] Though the technologies appear similar, they are polar opposites. The two use different vernacular, protocols, software, and hardware, and traditional IT generally serves people while OT serves devices.[171]

Perhaps the biggest roadblock to securing federal facility BAS is the lack of control the DHS and GSA have over the contractors currently maintaining most BAS networks. As previously stated, as of March 2015, approximately 300 federal facility BAS networks are housed on the GSA network, and protected behind the GSA firewall; the remaining facilities are operated on private contractor networks. While GSA is in the process of moving these facilities over to their network, until they do, these networks appear to be beyond the control of the government.

According to a 2014 GSA BAS upgrade contract solicitation, the government contractor ultimately awarded the contract was not required to disclose how many of their employees would have access to these networks or in what manner employees would access the network, whether or not risk assessments would be conducted, what, if any, intrusion detection software the company would use, or the effectiveness of the company's password management policies.[172]

---

169 U.S. Government Accountability Office, *Federal Facility Cybersecurity*.

170 Michael Chipley, "Cybersecurity: Introduction," Whole Building Design Guide, October 23, 2014, http://www.wbdg.org/resources/cybersecurity.php?r=secure_safe.

171 Ibid.

172 "Building Automation System Upgrade," Federal Business Opportunities, June, 24, 2014, https://www.fbo.gov/index?s=opportunity&mode=form&id=4a0d482d88af8b5b7f35b01eb837b024&tab=core&_cview=1.

The guide for facilities standards for the Public Building Service (PBS) of GSA describes design standards and "criteria for new buildings, repairs and alterations."[173] The guide describes GSA's desire to integrate BAS designs with other IT systems to "minimize costs and improve operations."[174] This decision increases opportunities for network intrusions due to the additional IT systems exposed to the BAS. However, it is encouraging that the standards require the project manager to coordinate with the PBS chief information officer (CIO) at the beginning of the building design process, potentially limiting future cybersecurity vulnerabilities related to BAS installation and monitoring.[175]

Another roadblock for the DHS is that it does not currently have sufficient technical expertise to assess these networks on a broad scale, nor investigate possible intrusions for eventual prosecution of bad actors, with the lone exception of the USSS.[176] ICS-CERT informed the author they have less than 30 personnel who are trained to respond to ICS network cybersecurity incidents and they lack law enforcement authority. Conversely, FPS has the necessary law enforcement authority and responsibility to protect federal facilities, yet lacks the technical expertise to perform cybersecurity duties.[177] Currently, the only DHS component with both law enforcement authority to conduct criminal investigations and ICS forensic expertise is the USSS.[178] However, the Secret Service is not currently conducting any investigative activity related to GSA-owned facility BAS network intrusions.

---

[173] General Services Administration, *Facility Standards for the Public Building Service* (PBS-P100 2015) (Washington, DC: General Services Administration, 2015) 11, http://www.gsa.gov/portal/mediaId/225771/fileName/2015_P100_FacilitiesStandards.action.

[174] General Services Administration, *Facility Standards for the Public Building Service*, 143.

[175] Ibid.

[176] Senate Committee on Appropriations, Subcommittee on Homeland Security, *Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future* (statement by Special Agent in Charge William Noonan, May 7, 2014.

[177] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 5, 18.

[178] *Fighting Fraud: Improving Information Security: Joint Hearing Before the House Subcommittee on Financial Institutions And Consumer Credit of the Committee on Financial Services*, 108th Cong., 1(2003) (statement of Tim Caddigan, Special Agent in Charge, Financial Crimes Division, United States Secret Service).

At the 2015 Central Ohio InfoSec Summit, FBI Supervisory Special Agent (SSA) Kevin Rojek said, "The weakest link in cybersecurity is the general workforce"; this remains true of the DHS and GSA employees as well.[179] As long as government employees operating on a government network continue clicking on malicious links and opening emails from unknown sources, government networks will remain vulnerable.[180] SSA Rojek, however, stated that, no matter how sophisticated your intrusion detection system is, a well-funded, committed adversary will compromise your network.[181] SSA Rojek's words foreshadowed the June 2015 discovery of arguably the greatest cyberattack perpetrated against the U.S. government.[182] The cyberattack was directed toward the U.S. Office of Personnel Management's (OPM), computer network.[183] It is worth noting the OPM headquarters is an FPS-protected facility. If the attack had been perpetrated against the GSA to possibly obtain sensitive blueprints of intelligence community facilities, attackers could have potentially gained access to the BAS networks housed on the GSA enterprise network.

B. CURRENT CYBERSECURITY LAW

In the early 1980s, a lack of necessary criminal laws that could hold cyber criminals accountable for their actions existed.[184] As a result, Congress created a new statute; 18, U.S.C Section 1030 (Fraud and Related Activity in Connection with Computers).[185] The law has been strengthened over the years through additional legislative action, most notably through the passage of the Computer Fraud and Abuse Act (CFAA) of 1986.[186] The provisions most applicable to a cyberattack perpetrated

---

[179] Kevin Rojek, "Current Cyber Threats: An Ever Changing Landscape," Presented at the Central Ohio Info Sec Summit, Columbus, OH, March 24, 2015.

[180] Rojek, "Current Cyber Threats."

[181] Ibid.

[182] Andy Greenberg and Kim Zetter, "Why the OPM Breach Is Such a Security and Privacy Debacle," *Wired*, June 11, 2015.

[183] Ibid.

[184] U.S. Department of Justice, *Prosecuting Computer Crimes* (Washington, DC: Office of Legal Education Executive Office for United States Attorneys), 1.

[185] Ibid.

[186] Ibid.

against a BAS network are related to accessing a government computer without authorization or exceeding authorized use, obtaining information from a government computer in furtherance of any criminal or tortuous act, trespasses on a government network, damages to a computer or information or threats to do the same, and conspiracy to commit any of these offenses.[187] This law would apply to any "bad actor," whether trusted insider or "hacktivist," who trespasses or actually enters the federal facility BAS network with or without actual damage being done to the network or connected systems.

Whether or not a private contractor working on behalf of the government is considered a "department or agency of the United States for the purposes of prosecution" "has not been addressed by any court."[188] However, Section 1030(a) (3) allows for the prosecution of those who trespass into government and nongovernment systems, if "such conduct affects that use by or for the Government of the United States."[189] Those subject to prosecution under 1030(a) (3) are not required to have actually obtained information; merely "taking a look" would violate the law. It appears that this provision would cover intrusions into the networks belonging to private companies GSA has contracted to manage some BAS networks.

The Cyber Security Enhancement Act (CEA) of 2002 increased penalties under CFAA for individuals whose "violation was intended to or had the effect of significantly interfering with or disrupting critical infrastructure; and whether the violation was intended to or had the effect of created a threat to public health or safety, or injury to any person."[190] Any attack on a federal facility BAS would inherently qualify for enhanced penalties under the CEA, potentially serving as a deterrent to trusted insiders and hacktivists.

---

[187] U.S. Department of Justice, *Prosecuting Computer Crimes*, 1–59.

[188] Ibid., 19.

[189] Ibid.

[190] Pub. L. No. 107-296 Stat. 2136 Sec. 225, 2, B, 7, 8.

C. RELEVANT DRAFT CYBERSECURITY LEGISLATION

The 114th Congress is currently considering several cybersecurity-related bills and amendments that could impact federal facility BAS network security. If signed into law, these pieces of legislation would force the implementation of many of the policy options offered in this thesis, as well as encourage the private contractors who currently control the majority of federal facility BAS networks to provide the necessary risk mitigation strategies without fear of legal action. Aspects of the bills and amendments likely to affect the policy recommendations offered in this thesis are summarized in this section.

H.R. 1731—National Cybersecurity Protection Act of 2015 (Introduced April 12, 2015)

> Requires DHS to deploy at no cost, capabilities to protect federal agency information and information systems, including technologies to continuously diagnose, detect, prevent, and mitigate cybersecurity risks involving such systems. Authorizes the DHS Secretary to access, and allows federal agency heads to disclose to the Secretary, information traveling to or from or stored on a federal agency information system, regardless of from where the Secretary accesses such information, notwithstanding any law that would otherwise restrict or prevent federal agency heads from disclosing such information to the Secretary.[191]

The Act would also allow a private entity to assist the secretary in carrying out such activities and provide liability protections.[192]

H.Amdt.100 to H.R.1731 (Introduced April 23, 2015)

> The Amendment ensures that federal agencies supporting cybersecurity efforts of private sector entities remain current on innovation; industry adoption of new technologies; and industry best practices as they relate to industrial control systems.[193]

S.754—Cybersecurity Information Sharing Act of 2015 (Introduced March 17, 2015)

"Permits private entities to monitor, and operate defensive measures to detect, prevent, or mitigate cybersecurity threats or security vulnerabilities on: (1) their own

---

[191] *National Cybersecurity Protection Act*, HR 1731, 114th Cong., 1st sess. (2015).

[192] Ibid.

[193] *H. Amdt. 100 to National Cybersecurity Protection Act, HR1731*, 114th Cong., 1st sess. (2015).

information systems; and (2) with authorization and written consent, the information systems of other private or government entities."[194] Authorizes such "entities to monitor information that is stored on, processed by, or transiting such monitored systems."[195] The Act "allows entities to share and receive indicators and defensive measures with other entities or the federal government. Requires recipients to comply with lawful restrictions that sharing entities place on the sharing or use of shared indicators or defensive measures."[196] The Act would also allow a "private entity to assist the secretary in carrying out such activities" provide liability protections.[197]

H.R.1560: Protecting Cyber Networks Act (Introduced March 24, 2015)

1. Permits private entities to monitor or operate defensive measures to prevent or mitigate cybersecurity threats or security vulnerabilities, or to identify the source of a threat, on: (1) their own information systems; and (2) with written authorization, the information systems of other private or government entities. Authorizes entities to conduct such activities on information that is stored on, processed by, or transiting such monitored systems

2. Allows non-federal entities to share and receive indicators or defensive measures with other non-federal entities or specifically designated federal entities, but does not authorize non-federal entities to share directly with components of the Department of Defense (DOD), including the National Security Agency (NSA). Allows otherwise lawful sharing by non-federal entities of indicators or defensive measures with DOD or the NSA. Requires recipients to comply with lawful restrictions that sharing entities place on the sharing or use of shared indicators or defensive measures

3. Requires the Small Business Administration (SBA) to provide assistance to small businesses and financial institutions to monitor information systems, operate defensive measures, and share and receive indicators and defensive measures. Directs the SBA to submit to the President a report regarding the degree to which small businesses and financial institutions are able to engage in such sharing. Requires the federal government to conduct outreach to encourage such businesses and institutions to engage in those activities.

---

194 *Cybersecurity Information Sharing Act*, S 754, 114th Cong, 1st sess. (2015).

195 Ibid.

196 *Cybersecurity Information Sharing Act*, S 754, 114th Cong, 1st sess. (2015).

197 Ibid.

4. Allows non-federal entities, for cybersecurity purposes, to share with other non-federal entities or the NCCIC any indicators or defensive measures obtained from: (1) their own information systems; or (2) the information systems of other federal or non-federal entities, with written consent. Authorizes non-federal entities (excluding state, local, or tribal governments) to conduct network awareness to scan, identify, acquire, monitor, log, or analyze information, or to operate defensive measures, on the information systems of entities that provide consent.

5. Establishes a private cause of action that a person may bring against the federal government if a federal agency intentionally or willfully violates restrictions on the use and protection of voluntarily shared indicators or defensive measures.[198]

S.456: Cyber Threat Sharing Act of 2015 (Introduced February 11, 2015)

1. Permits any entity to disclose lawfully obtained indicators to a federal entity for investigative purposes consistent with the lawful authorities of the federal entity. Restricts private entities' use, retention, or further disclosure of cyber threat indicators to purposes relating to information system protection, cyber threat identification or mitigation or crime reporting.

2. Prohibits a federal entity from using a disclosed indicator as evidence in a regulatory enforcement action against the entity that disclosed the indicator, but allows a federal entity to use disclosed indicators for regulatory enforcement if the information is received by other lawful means.[199]

H.R.234: Cyber Intelligence Sharing and Protection Act (Introduced January 8, 2015)

1. Permits any entity to disclose lawfully obtained indicators to a federal entity for investigative purposes consistent with the lawful authorities of the federal entity.

2. Restricts private entities' use, retention, or further disclosure of cyber threat indicators to purposes relating to information system protection, cyber threat identification or mitigation, or crime reporting.[200]

---

198 *Protecting Cyber Networks Act*, HR 1560, 114th Cong., 1st sess. (2015).

199 *Cyber Threat Sharing Act of 2015*, S 456, 114th Cong., 1st sess. (2015).

200 *Cyber Intelligence Sharing and Protection Act*, HR 234, 114th Cong., 1st sess. (2015).

H.R.53—Cyber Security Education and Federal Workforce Enhancement Act
Introduced January 6, 2015)

> Amends the Homeland Security Act of 2002 to establish within the Department of Homeland Security (DHS) an Office of Cybersecurity Education and Awareness Branch to make recommendations to DHS regarding: (1) recruitment of information assurance, cybersecurity, and computer security professionals; (2) grants, training programs, and other support for kindergarten through grade 12, secondary, and post-secondary computer security education programs; (3) guest lecturer programs in which professional computer security experts lecture computer science students at institutions of higher education; (4) youth training programs for students to work in part-time or summer positions at federal agencies; and (5) programs to support underrepresented minorities in computer security fields with programs at minority-serving institutions.[201]

D. THE ROLE OF GSA IN FEDERAL FACILITY BAS SECURITY

The GSA's business strategy is presumably linked to providing safe, secure, and cost-effective government facilities for federal agencies to carry out their work on behalf of the American people. The GSA business strategy should drive their organizational and information systems security strategy related to BAS, understanding that any strategy for one will have consequences for the others.[202] Currently, due to the lack of BAS network security protocols, the GSA's information systems security and organizational strategies do not support GSA's business strategy as described previously.[203]

In 2011, the GAO added federal real property management to its list of 30 areas it determined to be "high-risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement."[204] As of December 2014, BAS networks with network or Internet connections were installed in approximately 500 GSA-owned facilities, and the GSA has

---

201 *Cyber Security Education and Federal Workforce Enhancement Act*, HR 53, 114th Cong., 1st sess. 2015).

202 Keri E. Pearlson and Carol S. Saunders, *Managing and Using Information Systems*, 5th ed. (Hoboken, NJ: John Wiley and Sons, 2013), 23–32.

203 Ibid.

204 U.S. Government Accountability Office, *High-Risk Series: An Update* (GAO-13-283) (Washington, DC: U.S. Government Accountability Office, 2013), 106, http://www.gao.gov/assets/660/652133.pdf.

only conducted limited security assessments of 300 of these facilities.[205] The statistics regarding the number of facility BAS currently networked contained in the 2014 GAO report previously cited, differs from the numbers the GSA cited during a March 24, 2015 briefing at the Cybersecurity Building Control Systems Workshop held in Washington, DC.[206] One of the GSA representatives who presented at the Workshop was contacted to clarify the discrepancy but failed to respond to the author's inquiry.

The GSA recently communicated to the GAO that it is responsible for the networks that run BAS in their owned facilities; however, the GAO found that the GSA is not in compliance with FISMA.[207] While the GSA is conducting "security control" assessments of federal facility BAS, the assessments are not designed to assess the cybersecurity risks BAS face.[208] Additionally, the GSA only assessed the security controls of approximately 22 percent of their BAS-equipped facilities during a five-year period from 2009 to 2014.[209] Further, of the 110 GSA-produced security assessments reviewed by the GAO, only about 18 percent were in compliance with the NIST framework.[210] The GSA CIO explained that the GSA conducts their security assessments the way it does because the GSA's "approach to assessing cyber risk to these systems is evolving."[211]

The GSA's Building Technology Services' representatives told the Cybersecurity Building Control Systems Workshop in March 2015 that only three hundred of its facilities that employ BAS network technology are housed on the GSA network, and protected behind the GSA firewall.[212] The representatives revealed that the GSA is currently using 400 servers with 50 different pieces of software, and the devices and

---

[205] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 22.

[206] Mordin and Schadchehr, "Building Monitoring and Control Systems in GSA."

[207] Mordin and Schadchehr, "Building Monitoring and Control Systems in GSA."

[208] U.S. Government Accountability Office, *Federal Facility Cybersecurity:*

[209] Ibid.

[210] Ibid.

[211] Ibid., 23.

[212] Mordin and Schadchehr, "Building Monitoring and Control Systems in GSA."

software are not currently in compliance with federal security standards.[213] To address BAS security issues, the GSA established a Building Technology Services Program Management Office (BTSPMO) within the CIO's office, and created a security assessment process tailored to evaluate devices. The BTSPMO have assessed 150 unique devices and found that only 28 meet current GSA security standards.[214] It is unknown if GSA security standards are in compliance with DHS security standards.

Moving forward, the GSA has indicated the agency will begin utilizing DHS risk assessment software to assess vulnerabilities in its facilities that use networked BAS.[215] The GSA also plans to integrate the remaining buildings in its inventory, moving them from private-sector networks to the GSA network, protected behind the GSA firewall.[216] While it appears the GSA is moving in the right direction, their pace is slow. With no publicly acknowledged deadline for securing these networks, it is unknown how high a priority BAS network security is for the GSA.

E. THE ROLE OF DHS IN FEDERAL FACILITY BAS SECURITY

The Homeland Security Act of 2002 requires DHS to "protect federal facilities as well as people on the property."[217] However, a December 2014 GAO report found that "no one within DHS is assessing or addressing cyber risk to building and access control systems particularly at the nearly 9,000 federal facilities protected by FPS," reportedly "because cyber threats involving these systems are an emerging issue."[218] DHS's failure to assess the cyber risks to federal facilities appears to place them out of compliance with FISMA, as well as the National Cybersecurity Protection Act of 2014 (NCPA), and the Cybersecurity Workforce Assessment Act of 2014 (CWAA) . Although the time between the passage of those acts and the timing of this inquiry have been relatively short, DHS is also not in compliance with older E.O.s and presidential directives, namely E.O 13231,

[213] Mordin and Schadchehr, "Building Monitoring and Control Systems in GSA."

[214] Ibid.

[215] Ibid.

[216] Ibid.

[217] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 4.

[218] Ibid., 17.

PPD-21, or HSPD-23. These laws, directives, and E.O.s provide clear authorities, responsibilities, and mechanisms for DHS to secure federal facility BAS. Those authorities and responsibilities related to federal facility BAS networks are outlined in this section.

FISMA (2002)

- Required DHS to develop a plan to secure physical and technical assets that support U.S. critical infrastructure
- Provided DHS with a comprehensive framework to assess risk through NIST
- Required DHS secretary to create security controls to mitigate identified risks to information systems

NCPA (2014)

- Requires DHS to "develop, maintain, and exercise cyber incident response plans to address cybersecurity risks to critical Infrastructure."[219]

CWAA (2014)

- Requires the DHS secretary to assess if the DHS workforce is capable of meeting its cybersecurity mission

E.O. 13231 (2001)

- Required the DHS secretary to coordinate cyber incident and response
- Required federal government critical infrastructure information systems be secure

PPD-21 (2013)

- Requires DHS to secure critical infrastructure that supports DHS's primary mission

[219] *National Cybersecurity Protection Act of 2014.*

HSPD-23- (2008)

- Requires DHS intrusion detection program, EINSTEIN, be deployed to all federal systems to enhance system security
- Provides support for law enforcement capabilities

The NPPD is responsible ensuring the United States remains both secure and resilient with respect to physical and cyber-critical infrastructure from attacks (physical and cyber) and catastrophic incidents.[220] Security of federal facilities and federal information system networks are also the responsibility of NPPD.[221]

Housed within NPPD's National Cybersecurity and Communications Integration Center (NCCIC) is the Industrial Control Systems Cyber Emergency Response Team (ISC-CERT). The ISC-CERT provides on-site incident response to ICS-related incidents free of charge, conducts vulnerability, malware, and digital media analysis, offers mitigation strategies, provides situational awareness via actionable intelligence, coordinates "the responsible disclosure of vulnerabilities," and provides alerts and bulletins on threats and vulnerabilities to ICS.[222] However, these services are currently directed toward the private sector and federal facilities not protected by FPS. The ICS-CERT also directed the development of the Cyber Security Evaluation Tool (CSET).[223] The CSET is a free, downloadable, step-by-step risk assessment tool that any ICS owner/operator can use to assess their ICS network cybersecurity practices "against recognized industry standards."[224] The tool highlights system vulnerabilities and identifies best practices to be followed.[225]

---

[220] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 4.

[221] Ibid.

[222] "Homepage," Industrial Control Systems Cyber Emergency Response Team, June 14, 2015, https://ics-cert.us-cert.gov/.

[223] "CSET Homepage," Industrial Control Systems Cyber Emergency Response Team, June 14, 2015, https://ics-cert.us-cert.gov/sites/default/files/FactSheets/CSET%20Fact%20Sheet_20140528.pdf.

[224] Ibid.

[225] Ibid.

The Federal Protective Service (FPS), a subcomponent of NPPD, provides security and law enforcement services to over 9,000 facilities that are leased or owned by the government within the United Statesd .[226] FPS carries out its mission by conducting facility security assessments to assess federal facility security vulnerabilities, as well as threat assessments and law enforcement response, and investigative follow-up. The FSA documents federal facility security vulnerabilities on a recurring basis (on either a three- or five-year interval based on the facility security level of the facility being assessed).[227] FPS employs approximately 1,100 law enforcement and security professionals to accomplish their mission.[228] FPS law enforcement officers derive their authority from Title 40 United States Code, section 1315, and are tasked with conducting felony criminal investigations involving crimes such as possession of explosives, sexual assault, robbery, homicide, arson, weapons violations, threats, and theft.[229]

Although DHS does not currently have a strategy to secure federal facility BAS, NPPD has begun the process of understanding the cyber risks to federal facilities from facility BAS.[230] In 2013, FPS, NPPD's Office of Infrastructure Protection (IP), and ICS-CERT conducted a joint security assessment of a GSA-owned facility in Washington, DC, assessing both the physical and cyber vulnerabilities.[231] Also in 2013, FPS developed a discussion paper for the ISC that identified "the types of building systems that could be assessed for cyber risk, including heating, ventilation, and air conditioning;

---

[226] "The Federal Protective Service," U.S. Department of Homeland Security, June 13, 2015, http://www.dhs.gov/federal-protective-service-0.

[227] U.S. Government Accountability Office, *Homeland Security: The Federal Protective Service Faces Several Challenges That Hamper its Ability to Protect Federal Facilities* (GAO-08-683) (Washington, DC: U.S. Government Accountability Office, 2008), http://www.gao.gov/new.items/d08683.pdf.

[228] Ibid.

[229] U.S. Government Accountability Office, *Federal Law Enforcement: Results of Surveys of Federal Civilian Law Enforcement Components* (GAO-07-223SP) (Washington, DC: U.S. Government Accountability Office, 2006), http://www.gao.gov/products/GAO-07-223SP.

[230] U.S. Government Accountability Office. *Federal Facility Cybersecurity*, 16.

[231] Ibid.

access controls; closed-circuit video; fire annunciation panels; and security command and control centers."[232]

Despite the fact that PPD-21 clearly holds the GSA administrator responsible for the security of BAS networks inside GSA-owned facilities, DHS appears to be at least equally responsible. Both GSA and DHS are ISC working group members and, after the release of the 2014 GAO report on BAS network security, both now acknowledge their general responsibility to secure these networks. DHS agreed with the GAO recommendations and informed the GAO that NPPD's FPS, IP, and CS&C have agreed to "consult with GSA, the Interagency Security Committee (ISC) and other relevant federal agencies to develop a strategy for addressing cyber risk to building and access control systems."[233]

ICS-CERT is also working with other ISC members to "incorporate potential cyber risks to buildings and access control systems into the Design-Basis Threat Report."[234] The GSA administrator agreed with the recommendations offered by the GAO and will ensure, going forward, that the GSA's cyber risk assessments of its building control systems will be in compliance with FISMA.[235] Additionally, the GSA agreed to partner with DHS to "develop and implement a framework" for cyber risks.[236] Although it is encouraging that DHS and the GSA have acknowledged this problem and both accept responsibility for fixing it, it remains to be seen exactly how that solution will look.

F. EVALUATION CRITERIA

Each option offered throughout this inquiry was analyzed using five evaluative categories obtained from Naval Postgraduate School alumnus Todd Consolini, of the

[232] U.S. Government Accountability Office. *Federal Facility Cybersecurity*, 16.

[233] U.S. Government Accountability Office. *Federal Facility Cybersecurity*, Appendix III.

[234] Ibid.

[235] Ibid., Appendix IV.

[236] Ibid.

Center for Homeland Defense and Security.[237] Consolini, a supervisory physical security specialist employed by the FPS, wrote his master's thesis on innovative ways to enhance the physical security risk assessment process of federal facilities. Consolini's criteria and framework were used in this thesis because the drivers he identified in his policy recommendations are applicable to current DHS policymakers' sensitivities. These criteria are DHS acceptability, compliance (with laws, E.O.s, and presidential directives), implementation, effectiveness, and time.[238]

DHS acceptability is the probable level of acceptance across all DHS sub-components. An acceptability rating of low means the recommendation is not likely to be accepted by any DHS sub-component and a significant event will be necessary to gain acceptance.[239] An acceptability rating of medium means the recommendation is likely to be accepted by the DHS sub-component leadership, but may not be by the practitioners charged with carrying out instructions from leadership.[240] An acceptability rating of high means that the recommendation is expected to be accepted by both DHS sub-component leadership and practitioners.[241]

Compliance is the level at which the recommendation complies with laws, E.O.s, and directives. Non-compliant means the recommendation does not, in any way, conform to established laws. Partial compliance implies the recommendation follows only some laws, while compliant means the recommendation fully meets the requirements of all laws, E.O.s, and directives related to securing federal facility BAS.

Implementation refers to how difficult it may be to fully enact the recommendation across DHS. The analysis options are simple, somewhat difficult, or very difficult. A simple rating implies the recommendation will require virtually no additional personnel, training, or policy creation or revisions.[242] A somewhat difficult

---

[237] Consolini, "Regional Security Assessments."

[238] Ibid.

[239] Consolini, "Regional Security Assessments."

[240] Ibid.

[241] Ibid.

[242] Ibid.

rating means that some additional personnel, training (less than six months), and few policy creations or revisions would be necessary. A very difficult designation means the recommendation will require large numbers of additional personnel, extensive training (more than six months), and major policy creations or revisions.[243]

Effectiveness is the projected level of overall risk reduction associated with securing federal facility BAS.[244] This criterion is evaluates the option as having low, medium, or high levels of risk reduction.[245] A low level of risk reduction means the recommendation offers little to no improvement in federal facility BAS network security.[246] A medium designation implies the recommendation will improve BAS network security at facilities housed on the GSA network, protected behind the GSA firewall. A high ranking indicates the recommendation will increase security of BAS networks in all GSA-owned facilities, because contractor-controlled BAS networks are factored into the recommendation.

Time investment is the amount of time necessary for DHS to fully implement the recommendation. This is judged as requiring a minimal, minor, or major time commitment. A minimal time commitment means creation and employment are expected to take less than a year; minor means more than one year but less than two; major means more than two years.[247]

G. ANALYSIS OF OPTION I: MAINTAINING THE STATUS QUO

Option I is presented in this inquiry as maintaining the status quo. This option exists to be matched against the other options/recommendations to ascertain the ideal option for the DHS. Table 1 summarizes the analysis of current DHS practices against the categories.

---

[243] Consolini, "Regional Security Assessments."

[244] Ibid.

[245] Ibid.

[246] Ibid.

[247] Ibid.

Table 1. Status Quo (Option I) Evaluation

Option	DHS Acceptability	Compliance	Implementation	Effectiveness	Time
I	Low	Not in Compliance	Simple	Low	Minimal

(1) DHS Acceptability

DHS is currently not monitoring federal facility BAS networks or conducting risk assessments to determine the threats and vulnerabilities to these networks. However, DHS has agreed to develop a strategy to secure federal facility BAS that "defines the problem; identifies the roles and responsibilities; analyzes the resources needed, and identifies a methodology for assessing cyber risk to building and access control systems."[248] Therefore, the acceptability rating for Option I is low.

(2) Compliance

Because DHS does not currently conduct cybersecurity assessments of federal facility BAS, the Department is not in compliance with portions of at least three federal laws and at least three E.O.s and directives. As such, the DHS is assessed as not in compliance.

(3) Implementation

DHS is not currently involved in BAS network security for federal facilities; as there is nothing yet to actually implement, the implementation rating is simple.

(4) Effectiveness

DHS has failed to address cybersecurity concerns of federal facility BAS, and therefore has a low level of effectiveness in terms of reducing risks within BAS networks.[249]

[248] U.S. Government Accountability Office, *Federal Facility Cybersecurity*, 16.

[249] Consolini, "Regional Security Assessments."

(5) Time

There is no publicly available information about DHS developing a strategy to secure BAS networks inside federal facilities. Time investment is assessed as minimal.

H. OVERALL ANALYSIS

Congress and the president have granted DHS clear authorities to protect federal facility BAS; however, the Department is still not monitoring or assessing the cyber risks to these facilities, and as such is not compliant with federal laws or presidential E.O.s and directives. Now that DHS has acknowledged its role in securing these networks, significant roadblocks remain—chiefly, that, after DHS develops a comprehensive strategy to secure these networks, the vast majority of them are currently controlled by private sector contractors.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. OPTION II—LEVERAGING EXISTING DHS CAPABILITIES

A. OPTION II OVERVIEW

DHS possesses a broad array of cyber security expertise and authorities that have evolved since the Department's creation 12 years ago. DHS has developed its own intrusion detection software for federal information systems, created emergency response teams that can deploy to cybersecurity incidents on short notice, established a national integration center to share cyber-threat information, and joined the National Cyber Investigative Joint Taskforce (NCIJTF). However, DHS has not effectively incorporated its component and sub-component law enforcement authorities in its cyber mission. This chapter analyzes the existing capabilities the DHS possesses to determine if they are sufficient to secure federal facility BAS.

Option II recommends leveraging existing DHS capabilities to defend against threat actors. DHS can employ ICS-CERT to conduct risk assessments and respond to cyber intrusions, and can deter future cyber threat actors by asking the USSS to conduct criminal investigations into intrusions (investigative findings can be forwarded to the Department of Justice for prosecution). DHS's ICS-CERT should utilize their Cyber Security Assessment Tool (CSET) to conduct an initial assessment of federal facilities to determine if their BAS networks are in compliance with the NIST framework. DHS should also leverage ICS-CERT's expeditionary capability to conduct risk assessments and incident response remotely, saving the significant cost associated with field deployments.

Additionally, the DHS intrusion detection system (IDS), EINSTEIN, is presumably deployed on the GSA network; however, no references to the actual agencies utilizing EINSTEIN were located in the available research. While this thesis speculates EINSTEIN is protecting the 300 BAS currently on the GSA network, it is unconfirmed.[250] The USSS has the technical expertise, equipment, and experience to

[250] Mark Rockwell, "New BPAs to Aid in Cyberdefense," FCW, August 14, 2013, http://fcw.com/articles/2013/08/14/dhs-cmaas.aspx?m=1.

conduct intrusion investigations, gained through the work of their Critical Systems Protection Program (CSP). The CSP could leverage its many agents in field offices throughout the country to respond to reported intrusions on federal facility BAS networks. Option II would also integrate law enforcement response and investigative follow-up with current ICS-CERT responsibilities, largely consisting of assessing risk and preventing intrusions.

B. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

To analyze both classified and unclassified vulnerabilities and threats, and coordinate findings with partner agencies to reduce risk to critical infrastructure, DHS established the National Cybersecurity and Communications Integration Center (NCCIC).[251] The NCCIC is "a 24x7 cyber situational awareness, incident response, and management center" housed within NPPD's Office of Cybersecurity and Communications.[252] Both the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT), as well as the National Coordinating Center for Communications are located within the NCCIC. The NCCIC is the "national nexus of cyber and communications integration for the federal government, intelligence community and law enforcement."[253] By leveraging the Center and its capabilities to secure federal facility BAS, the DHS would appear to have a significant cybersecurity "force-multiplier"; however, that may not be the case.

In December 2014, President Obama signed into law the National Cybersecurity Protection Act (NCPA) of 2014. The Act amends the Homeland Security Act of 2002 to codify into law the existing NCCIC to "carry out responsibilities of the DHS Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and

---

[251] Larry Zelvin, "National Cybersecurity & Communications Integration Center (NCCIC) Overview," Presented at the Information Security and Privacy Advisory Board, Washington, DC, October 12, 2012.

[252] "About The National Cyber Security and Communications Integration Center," U.S. Department of Homeland Security, June 16, 2015, http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

[253] "About The National Cyber Security and Communications Integration Center," U.S. Department of Homeland Security.

related DHS programs."[254] The Center shares real-time information on cybersecurity analysis, risks, incidents, and warnings for both the federal government and private sector across federal and non-federal platforms. However, due to the classified nature of the majority of the Center's work, it is publicly unknown how effective the Center actually is.

In August 2015, Nextgov, an "information resource for federal technology decision makers," claimed that 75 percent of the NCCIC's critical infrastructure sector analyst positions at the Center were vacant.[255] Nextgov revealed that 11 critical infrastructure sectors did not deploy their analysts physically at the Center, leaving only four sectors represented. Nextgov speculated that these vacancies exist because private sector CI operators do not want to expend the resources to place employees outside of their organization. Further, it was revealed that DHS does not currently have the funds to sponsor private-sector participation.[256] Also cited in the article was the private sector's dissatisfaction with the time it takes to obtain security clearances and the cell phone security restrictions on employees assigned to the NCCIC, preventing them from communicating emerging cyber threats with their parent organizations in a timely manner.[257]

Additionally, U.S. Senator Tom Coburn released a report in January 2015 titled, "A Review of the Department of Homeland Security's Missions and Performance."[258] Along with an inadequate level of participation, the report found that DHS is not leveraging all of the Center's assets. The Coburn report also cited a 2013 DHS OIG

---

[254] *National Cybersecurity Protection Act of 2014*, 128.

[255] Aliya Sternstein, "The Nation's 24-Hour Cyber Watch Center Still Has Some Empty Seats," NextGov, August 24, 2015, http://www.nextgov.com/cybersecurity/2015/08/nations-24-hour-hack-watch-center-missing-three-quarters-industry/119392/?oref=govexec_today_nl.

[256] Ibid.

[257] Ibid.

[258] Tom Coburn, "A Review of the Department of Homeland Security's Missions and Performance," U.S. Senate Committee on Homeland Security & Governmental Affairs, January 2015, file:///C:/Users/abhousto/Downloads/Senator%20Coburn%20DHS%20Report%20FINAL.pdf.

report claiming the NCCIC "struggled with sharing cyber information among the federal cyber operations centers."[259]

Industrial Control Systems-Cyber Emergency Response Team

The ICS-CERT enjoys vast awareness of the cyber-risk landscape through their coordination with both private-sector and international computer emergency response teams (CERTs). Additionally, ICS-CERT's Advanced Analytical Laboratory (AAL) provides research and analysis capabilities in support of ICS-CERT's assessment and incident response activities.[260] The AAL has developed a forensic suite called the Analyst Network Tool that uses commercial and forensic tools; this suite has the capability to process multiple drive images, "reducing the amount of analyst hands-on time."[261] ICS-CERT has developed three training courses to help those responsible for ICS network security have more awareness of the risks associated with ICS. The first two training courses are available online and the third is a five-day, in-person, hands-on technical-level course.[262]

In 2014, ICS-CERT responded both remotely and on-site to 245 cybersecurity incidents for control systems throughout the country to provide incident response support and mitigation strategies; approximately 13.5 percent of the incidents were linked to the Government Facilities Sector (GFS).[263] However, from 2012 to 2014, ICS-CERT only provided on-site incident response on 17 occasions.[264] This may be due to the limited number of personnel ICS-CERT employs, although, during the same period, they conducted 265 on-site risk assessments, with 104 in 2014 alone.[265] The capabilities ICS-CERT could bring to improve security of federal facility BAS are immense. ICS-CERT

---

[259] Tom Coburn, "A Review of the Department of Homeland Security's Missions and Performance."

[260] Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Year in Review 2015*, (Washington, DC: U.S. Department of Homeland Security, 2015), 9, https://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2014_Final.pdf.

[261] Ibid.

[262] Ibid., 12.

[263] Ibid.

[264] Ibid., 19.

[265] Ibid.

can use their Cyber Security Evaluation Tool (CSET) to conduct initial assessments of BAS networks, and leverage the AAL, provide on-site and remote incident response if required, and provide risk assessments.

C. NETWORK PROTECTIVE METHODS

When deployed properly, IDS can "provide warnings indicating that a system is under attack, even if the system is not vulnerable to the specific attack."[266] Despite cybersecurity researchers' best efforts, however, IDS technology is "immature and its effectiveness limited."[267] ICS network security programs are encouraged to follow, as the NIST SP 800–82 suggests, a "defense-in-depth" approach. A defense-in-depth approach protects a network with several mechanisms; if one fails, others will be in place to stop the attack.268 Once an IDS is deployed, provisions must also be made to monitor the system to ensure adequate response.[269] IDS are designed to passively detect incoming or outgoing traffic linked to known malware signatures (Trojans, viruses, "worms, and other dangerous code").[270] Intrusion prevention systems (IPS) use IDS but enhance its detection capabilities with action that can be programmed to block intrusions based on specific signatures.[271] As a result, IDS/IPS can only stop attacks of known bad signatures, making them useless against new or unique signatures.

A typical ICS defense-in-depth strategy, as described in NIST SP-800-82, includes:

- Developing security policies, procedures, training and educational material that applies specifically to the ICS

---

[266] John McHugh, Alan Christie, and Julia Allen, "Defending Yourself: The Role of Intrusion Detection Systems," 17, no. 5 (September/October 2000): 42–51, https://nps.illiad.oclc.org/illiad/illiad.dll?Action=10&Form=75&Value=144466.

[267] Ibid.

[268] "InfoSec Reading Room," SANS Institute, last modified October 28, 2015, http://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525.

[269] McHugh, Christie, and Allen, "Defending Yourself," 47.

[270] Andreas Kuehn and Milton Muelller, "Securitizing Critical Infrastructure, Blurring Organizational Boundaries: The U.S. Einstein Program," 5, presented at the Research Conference on Communication, Information and Internet Policy, Arlington, VA, September 29, 2013.

[271] Ibid.

- Considering ICS security policies and procedures based on the Homeland Security Advisory System Threat Level, deploying increasingly heightened security postures as the Threat Level increases

- Addressing security throughout the life cycle of the ICS from architecture design to procurement to installation to maintenance to decommissioning

- Implementing a network topology for the ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.

- Providing logical separation between the corporate and ICS networks (e.g., stateful inspection firewall(s) between the networks, unidirectional gateways)

- Employing a DMZ network architecture (i.e., prevent direct traffic between the corporate and ICS networks)

- Ensuring that critical components are redundant and are on redundant networks.

- Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events

- Disabling unused ports and services on ICS devices after testing to assure this will not impact ICS operation

- Restricting physical access to the ICS network and devices

- Restricting ICS user privileges to only those that are required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege)

- Using separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts)

- Using modern technology, such as smart cards for Personal Identity Verification (PIV)

- Implementing security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS

- Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications where determined appropriate

- Expeditiously deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the ICS
- Employing reliable and secure network protocols and services where feasible[272]

1. National Cybersecurity Protection System

The National Cybersecurity Protection System, known as EINSTEIN, was initially released in 2004 as a voluntary network surveillance program for government agencies.[273] In 2007, under the direction of OMB, DHS developed the Trusted Internet Connection (TIC) Program to restructure U.S. government networks for the purpose of making them more secure.[274] The GSA administers the TIC Program for the federal government.[275] To date, only four companies (AT&T, Qwest, Sprint, and Verizon) have undergone the TIC compliance validation process.[276] Prior to TIC, federal agencies could transact their own Internet services.[277]

Subsequent upgrades to EINSTEIN II in 2008 included IDS capability, and in 2014 DHS awarded a contract to CenturyLink to include IP capabilities in EINSTEIN III, due to be released in December 2015.[278] EINSTEIN III will reportedly be capable of conducting advanced email filtering, spoofing protections, and mitigation and prevention services to participating federal agencies.[279] Recently, the Assistant Secretary of the Office of Cybersecurity and Communications (CS&C), Andy Ozment, told a Senate committee that 51 federal agencies have signed memorandums of agreement (MOA) to

---

[272] Stouffer, *NIST Briefing: ICS Cybersecurity Guidance*, 4.

[273] Kuehn and Muelller, "Securitizing Critical Infrastructure," 9.

[274] U.S. Government Accountability Office, *Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections At Federal Agencies* (GAO-10-237) (Washington, DC: U.S. Government Accountability Office, 2010), 2.

[275] Ibid.

[276] "Trusted Internet Connections (TICS)," U.S. General Services Administration, last modified March 25, 2015, http://www.gsa.gov/portal/content/104213.

[277] Kuehn and Muelller, "Securitizing Critical Infrastructure," 10.

[278] "CenturyLink Awarded New DHS EINSTEIN 3 Accelerated Task Order," CenturyLink, December 8, 2014, http://news.centurylink.com/news/centurylink-awarded-new-dhs-einstein-3-accelerated-task-order.

[279] Ibid.

have EINSTEIN III installed on their networks.[280] According to the MOA, CS&C provides signers of the MOA all labor, hardware, and software to deploy and operate EINSTEIN at no cost to the receiving agency.[281] However, EINSTEIN is not cheap; DHS requested $479.8 million to deploy the system on federal networks for FY2016.[282]

Additionally, the GAO has identified problems with the software's performance and capabilities; EINSTEIN's ability to detect signature anomalies is weak, and the new version of EINSTEIN uses only one of three NIST-identified detection methodologies.[283] The GAO also discovered that EINSTEIN is "only able to proactively mitigate threats across a limited subset of network (i.e., Domain Name System traffic and email)."[284] EINSTEIN deployment was another area the GAO found needed improvement. The GAO identified individual agency "implementation and policy challenges" for the limited number of federal agencies currently using EINSTEIN.[285]

As previously stated, IDS effectiveness is limited. While details are still emerging regarding the hacking method used in the devastating 2015 hack of OPM government employee files, DHS Spokesman S.Y. Lee said EINSTEIN was involved in discovering the breach.[286] DHS Cybersecurity Consultant Morgan Wright contends, however, that EINSTEIN failed to work properly because it took five months to discover the intrusion.[287] It should be noted that OPM did not have the current version of EINSTEIN

---

[280] *From Protection to Partnership: Funding the DHS Role in Cybersecurity, U.S. Senate*, 114th Cong., (2015) (statement of Andy Ozment, Assistant Secretary for NPPD Office of Cybersecurity & Communications).

[281] "Memorandum of Agreement Between the Department of Homeland Security, Office of Cybersecurity & Communications and _____," U.S. General Services Administration, last modified March 25, 2015, www.gsa.gov/portal/getMediaData?mediaId=169487.

[282] Sean Lyngass, "Security Experts: OPM Breach Show Einstein isn't Enough," *The Business of Federal* Technology," June 5, 2015, http://fcw.com/articles/2015/06/05/opm-einstein.aspx.

[283] U.S. Government Accountability Office, *Information Security: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies* (GAO-15-758T) (Washington, DC: U.S. Government Accountability Office, 2015), 16, http://www.gao.gov/assets/680/671253.pdf.

[284] Ibid.

[285] Ibid.

[286] David Sanger, "Hack Linked to China Exposes Millions of U.S. Workers," *New York Times*, June 4, 2015, http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html?_r=0.

[287] Lyngass, "Security Experts."

(EINSTEIN III) installed on its network at the time of the attack.[288] Previous versions of EINSTEIN were only capable of "identifying abnormal network traffic and detection known malicious traffic."[289] DHS Assistant Secretary for the Office of Cybersecurity and Communications Andy Ozment recently told Congress that the current version of EINSTEIN, EINSTEIN IIIA, is "like a guard post, capable of blocking prohibited users from accessing a network."[290] If OPM had been using the latest version of EINSTEIN, it appears the hack may never have happened.

2. Cyber Security Evaluation Tool (CSET)

CSET was developed under the direction of ICS-CERT to provide ICS owners and operators with a repeatable and systematic method for conducting assessments against several accepted standards and security practices, such as the NIST cybersecurity framework for ICS (SP-800-82).[291] CSET is a free-of-charge desktop software tool that can be used by "any organization to assess the security posture of cyber systems that manage a physical process or enterprise network," like a federal facility BAS.[292] The tool employs a user-friendly, question-and-answer format, much like the FPS Modified Infrastructure Survey Tool, which FPS uses to assess the physical security vulnerabilities of federal facilities. ICS-CERT has also made online tutorial videos that demonstrate how to use the tool, and will conduct on-site training to approved persons.[293]

Although CSET provides an initial starting point to establish a baseline security posture of a BAS, it does have limitations.[294] For example, CSET does not allow for detailed review of software and hardware configurations or detailed network architectural

---

[288] Mohana Ravindranath, "Committee Grills DHS Official Over Einstein's Failure To Prevent OPM Attack," NextGov, June 24, 2015, http://www.nextgov.com/cybersecurity/2015/06/house-committee-grills-dhs-official-failure-einstein-cdm-prevent-opm-attack/116242/.

[289] Ibid.

[290] Ibid.

[291] "CSET Frequently Asked Questions," U.S. Department of Homeland Security, accessed June 18, 2015, https://ics-cert.us-cert.gov/CSET-FAQ.

[292] Ibid.

[293] Ibid.

[294] "CSET Frequently Asked Questions," U.S. Department of Homeland Security.

analysis.[295] It must be noted, also, that CSET is a cybersecurity evaluation tool and, as such, does not evaluate risk.[296] With cyber threats facing ICS evolving almost daily, CSET is not enough to protect federal facility BAS, but is a starting point to begin the process. Earlier this year, the GSA expressed interest in utilizing CSET as part of their future assessments of federal facility BAS.[297]

D. UNITED STATES SECRET SERVICE CRITICAL SYSTEMS PROTECTION PROGRAM

Previously under the Department of Treasury, the USSS moved to the new Department of Homeland Security as a result of the Homeland Security Act of 2002.[298] Since the USSS moved to DHS they have expanded their involvement in cybersecurity significantly. Since 2003, the USSS Electronic Crimes Task Forces, consisting of federal, state, and local law enforcement agencies, expanded to twelve cities.[299] The USSS also established the Critical Systems Protection Initiative (CSPI), which leverages USSS cyber investigative trained personnel to support the Agency's mission at protected venues.[300] The CSPI was successfully used to secure the 2002 Salt Lake Olympics.[301] The Secret Service derives their authority to investigate cybercrime from Title 18 Section 1030 of the Computer Fraud and Abuse Act of 1986.[302] In 2008, the USSS established the National Computer Forensics Institute, where they train state and local law

295 "CSET Frequently Asked Questions," U.S. Department of Homeland Security.

296 Ibid.

297 Sandy Shadchehr and Josh Mordin, "Building Monitoring and Control Systems in GSA," presented at the Cybersecurity Building Control Systems Workshop, Washington, DC, March 24, 2015.

298 *An Act to Establish the Department of Homeland Security, and for Other Purposes (Homeland Security Act) Act of 2002*, Pub. L. No. 107-296, Stat. 2135 (2002).

299 Edward W. Lowery, "Closing the Cyber Gap: Integrating Cross-Government Cyber Capabilities to Support the DHS Cyber Security Mission" (master's thesis, Naval Postgraduate School, 2014), 74.

300 Ibid., 73.

301 Ibid., 73.

302 *Fraud and Related Activity in Connection with Computers*, 18 U.S.C. 1030, U.S. Criminal Code, Title 18, 1984, http://www.gpo.gov/fdsys/granule/USCODE-2010-title18/USCODE-2010-title18-partI-chap47-sec1030/content-detail.html.

enforcement, free of charge, on such topics as cybercrime trends and investigative methods.[303]

In 2004, the USSS partnered with the Carnegie Mellon University to conduct a study on the insider threat of "illicit cyber activity in the Banking and Finance Sector."[304] The study revealed that "behavioral approaches and security techniques could be effective in lessening an entity's exposure to threats from the cyber world." The study further found that, "1.) Most intrusions required little to no sophistication; 2.) Most intrusions were financially motivated; and 3.) Incidents were often uncovered by different entities but were rarely discovered by the victim."[305]

In 2010, the USSS established the Critical Systems Protection (CSP) program to support their protective mission. From 2010 to 2014, the USSS CSP program successfully completed more than 657 domestic and five international protective advances of venues the president, vice president, and other USSS protectees visited.[306] The CSP program's technology "gives the Secret Service the ability to identify cyber-threat actors, as well as mitigate the potential impact of a network attack on a protective venue or on the critical infrastructure that supports the venue."[307]

The Secret Service, as the lone DHS entity with law enforcement authority to investigate cyber intrusions, has access to a wealth of information and resources and is in a unique position to assist or lead criminal investigations into network intrusions. The National Cyber Investigative Joint Task Force (NCIJTF) is an FBI-led task force created in January 2008 by HSPD-23, and is responsible for "coordinating, integrating, and sharing pertinent information related to cyber threat investigations."[308]

---

303 "National Computer Forensic Institute Homepage," United States Secret Service, accessed June 18, 2015, https://www.ncfi.usss.gov/ncfi/pages/about.jsf;jsessionid=+vrHq3hgwno7QSmSkZ3mHtUw.

304 Lowery, "Closing the Cyber Gap," 75.

305 Ibid.

306 Senate Committee on Appropriations, Subcommittee on Homeland Security, *Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future* (statement by Special Agent in Charge William Noonan, May 7, 2014).

307 Ibid., 2.

308 National Security Council, *Cybersecurity Policy*, 9.

E. ANALYSIS AGAINST EVALUATION CRITERIA

As stated in Chapter III, each option is analyzed using five categories. These categories are DHS acceptability, compliance, implementation, effectiveness, and time.[309] Table 2 summarizes the analysis of Option II against these categories.[310]

Table 2. Option II Evaluation

Option	DHS Acceptability	Compliance	Implementation	Effectiveness	Time
II	Medium	Partially Compliant	Somewhat Difficult	Medium	Minor

(1) DHS Acceptability

The acceptability rating for Option II is averaged at medium. There are two entities charged with carrying out Option II; ICC-CERT received a rating of low and the USSS received a rating of high. While DHS headquarters leadership may be accepting of Option II, NPPD leadership may feel slighted; by allowing the Secret Service to conduct incident response and investigative follow-up, Option II completely removes the Federal Protective Service—a sub-component of NPPD with law enforcement investigative authority—from the strategy.

ICS-CERT employees would most likely welcome the use of CSET in federal facility assessments; however, Option II is not expected to be accepted by the employees of ICS-CERT.[311] By incorporating a law enforcement element to what has traditionally been a mitigation and assessment operation, ICS-CERT runs the risk of alienating their largest customer: the private sector. They have built a relationship of trust and discretion, and it is likely that private sector ICS critical infrastructure owners and operators would hesitate to report an intrusion to ICS-CERT if they feared the report could one day find

[309] Consolini, "Regional Security Assessments."

[310] Ibid.

[311] Consolini, "Regional Security Assessments."

its way into a courtroom. Despite the fact that law enforcement would only investigate intrusions into federal networks, the perception could persist.

Although the acceptability rating for ICS-CERT is judged as low, due to the recent increase of USSS involvement with cyber-related activities and investigations, Secret Service acceptability rating is judged as high because of the additional resources and expanded authority their involvement would likely foster. Both managers and employees would likely see this as an opportunity to improve their public image as well as to fine-tune skills used to protect private sector critical infrastructure sites under their umbrella. The expenses incurred by the Secret Service would likely be minimal due to the large number of available cyber-trained agents deployed throughout the country. The pre-existing framework the Secret Service utilizes for private sector critical infrastructure ICS assessments would also likely save funds. Finally, since the USSS was transferred to DHS, the agency has had some difficulty integrating within DHS; Option II encourages their integration.[312]

(2) Compliance with Laws, Presidential Executive Orders, and Directives

Option II is partially compliant with FISMA because it provides a plan to secure the physical and technical assets that support U.S. critical infrastructure.[313] It is compliant with the NCPA because it provides for a cyber-incident response plan. Option II may be partially compliant with HSPD-23 because EINSTEIN may be protecting federal facility BAS deployed on the GSA network, but not those housed on contractor-owned networks. Option II is compliant with PPD-21 because it provides cyber incident response coordinated through ICS-CERT and USSS. The USSS is assessed to be compliant with Title 18 Section 1030, which authorizes the agency to conduct criminal investigations into cyber intrusions of federal facility BAS networks.

[312] Lowery, "Closing the Cyber Gap," 72.

[313] Consolini, "Regional Security Assessments."

(3) Implementation

Implementation of Option II is assessed as somewhat difficult.[314] First, a memorandum of agreement would need to be signed between NPPD and USSS outlining roles and responsibilities for each. Both ICS-CERT and USSS would be required to write policies covering this new mission area; however, by leveraging existing related policies, this would not be a major undertaking. No significant training should be required for existing personnel. However, expanding ICS-CERT's role to include initial and continual network security assessment would require a moderate human capital investment to ensure existing capabilities are not degraded. In these times of federal budget austerity, it is unknown if NPPD would be able to support an expansion of its workforce for a threat that has not yet knowingly occurred in a federal facility.

(4) Effectiveness

Option II has a medium level of effectiveness in terms of risk reduction.[315] By incorporating a strategy that involves reoccurring risk assessment and incident response, as well as investigative follow-up of federal facility network intrusions, DHS is fulfilling its obligation to protect the cyber networks of critical infrastructure. However, this strategy would only affect roughly a quarter of the facilities owned by the GSA, and none of the commercial facilities the GSA leases from the Commercial Facilities Sector (CFS).

(5) Time

Option II is assessed as requiring a minor time investment.[316] The development of policies by ICS-CERT and USSS, as well as MOAs signed by both, are expected to take less than a year. However, the recruitment and training associated with new personnel for this new ICS-CERT mission is expected to take more than a year, but less than two.

[314] Consolini, "Regional Security Assessments."

[315] Ibid.

[316] Consolini, "Regional Security Assessments."

F. OVERALL ASSESSMENT

Option II would provide DHS with a relatively quick alternative to the status quo, and is assessed to be generally accepted by the DHS headquarters leadership and fully implementable in less than two years. While Option II cannot secure all federal facility BAS, it is a starting point. However, Option II does not take into account the mass exodus of USSS personnel every four years from their field offices to support presidential campaign protection. How DHS could overcome the gap in cyber incident response due to the void of deployed USSS personnel has not been assessed.

THIS PAGE INTENTIONALLY LEFT BLANK

V. OPTION III: CREATING A CYBERSECURITY DIVISION INSIDE THE FEDERAL PROTECTIVE SERVICE

A. OVERVIEW OF OPTION III

The Federal Protective Service (FPS) deploys a small, yet diverse and geographically dispersed, workforce focused on providing law enforcement and security services to protect federal facilities.[317] FPS is responsible for conducting physical risk assessments of federal facilities as well as criminal investigations into crimes occurring on federal property.[318] Backed by law and presidential E.O.s and directives, as well as provisions in the NIPP, FPS has clear authority to adopt the mission of securing federal facility BAS networks. Currently, however, FPS lacks the expertise to carry out this responsibility.[319]

Option III recommends that FPS leverage its existing risk management strategies (including those through ICS-CERT) and FPS' general criminal investigative techniques. Supplemented with new cybersecurity training, FPS could establish a cybersecurity capability to secure federal facility BAS networks. The roles and responsibilities associated with this new division are quite similar to existing FPS roles and responsibilities—namely, facility security assessments, continuous risk and threat assessment of federal facilities, and investigative response to crimes occurring on federal facilities. Significant challenges, however, such as recruitment and training for this undertaking, require a long-term commitment.

B. HISTORY OF THE FEDERAL PROTECTIVE SERVICE

The FPS traces its lineage back to the 1700s, when President George Washington appointed "three commissioners to establish a federal territory for a permanent seat of the

---

[317] U.S. Government Accountability Office, *Federal Protective Service: Protecting Federal Facilities Remains a Challenge* (GAO-14-623T) (Washington, DC: U.S. Government Accountability Office, 2014), 1.

[318] Shawn Reese and Lorraine H. Tong, *Federal Building and Facility Security* (CRS Report No. R41138) (Washington, DC: Congressional Research Service, 2010), https://www.fas.org/sgp/crs/homesec/R41138.pdf.

[319] U.S. Government Accountability Office. *Federal Facility Cybersecurity*, 17.

Federal Government"; an additional six night watchmen were ordered to protect the buildings the government would occupy.[320] Moving forward, the Act of June 1, 1948 created the General Services Administration (GSA) and, in the process, authorized the GSA to appoint special policemen to monitor all "buildings and areas owned or occupied by the United States and under charge and control of GSA."[321] These special policemen performed duties such as rendering first aid, answering visitor questions, and working fixed posts.[322] Over time, these duties would be transferred to FPS-managed contract security guards, now known as protective security officers (PSOs), of whom there are approximately 15,000.[323]

In the late 1960s and early 1970s, several federal facilities were attacked and damaged by bombings, disrupting functions of government.[324] These incidents likely contributed to the GSA administrator's decision to, in 1971, formally create the FPS through Administrative Order 5440.46.[325] From the 1970s to the 1990s, FPS generally served as a proactive police force for federal facilities. After the April 19, 1995 truck bombing of the Alfred P. Murrah Federal Building in Oklahoma City, which killed 168 men, women, and children, federal facility security was under scrutiny.[326]

As described in Chapter I, President Clinton ordered a complete review of federal facility physical security in the aftermath of the Oklahoma City bombing, which required all federal executive branch agencies to upgrade security at their facilities to ensure

---

320 *Federal Protective Service Reform Act of 2000*, HR 106-676, 106th Cong.,2nd sess. (2000). http://www.gpo.gov/fdsys/pkg/CRPT-106hrpt676/html/CRPT-106hrpt676.htm.

321 Ibid.

322 Ibid.

323 U.S. Government Accountability Office, *Homeland Security: Federal Protective Service's Use of Contract Guards Requires Reassessment and More Oversight* (GAO-10-614T) (Washington, DC: U.S. Government Accountability Office, 2010), 1, http://www.gao.gov/new.items/d10614t.pdf.

324 Keith Preston, *Attack the System: A new anarchist Perspective for the 21st Century* (London: Black House Publishing, 2013), 464–465.

325 *Federal Protective Service Reform Act of 2000*.

326 U.S. Department of Justice, *Vulnerability Assessment of Federal Facilities* (Washington, DC: U.S. Department of Justice, 1995), Introduction, https://www.ncjrs.gov/pdffiles1/Digitization/156412NCJRS.pdf.

compliance with newly established minimal standards.[327] Although federal facilities likely employed BAS at the time of the bombing, these systems were not connected to the Internet until several years later. As such, no technical security measures were assessed. The GSA was "also required to establish building security committees for all its facilities," which were later renamed facility security committees.[328] These committees meet on an as-needed basis to discuss security-related matters, such as whether or not existing countermeasures are sufficient. On October 19, 1995, the Interagency Security Committee (ISC) was established through Executive Order 12977.[329] The ISC was chaired by the GSA administrator until 2003, when the chairmanship transferred to the secretary of DHS.[330]

C. FPS AUTHORITY AND JURISDICTION

In 2002, the Homeland Security Act transferred FPS to the newly created Department of Homeland Security, where it was designated as part of Immigration and Customs Enforcement.[331] The Act also transferred the responsibility for federal facility security from the GSA to DHS.[332] The Act required the secretary of DHS to "protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government."[333] FPS derives its law enforcement authority from Title 40 U.S.C, Section 1315.[334] FPS law enforcement officers are authorized to

- (A) enforce federal laws and regulations for the protection of persons and property;
- (B) carry firearms;

---

[327] Reese and Tong, *Federal Building and Facility Security*, 1.

[328] Ibid.

[329] Executive Order 12977, "Interagency Security Committee," 60 *Federal Register* 54411–54412, October 24, 1995, 54412.

[330] U.S. Government Accountability Office, *Homeland Security: Further Actions Needed*, 9.

[331] *Homeland Security Act of 2002*.

[332] Ibid.

[333] Ibid.

[334] Ibid.

- (C) make arrests without a warrant for any offense against the United States committed in the presence of the officer or agent or for any felony cognizable under the laws of the United States if the officer or agent has reasonable grounds to believe that the person to be arrested has committed or is committing a felony;
- (D) serve warrants and subpoenas issued under the authority of the United States;
- (E) conduct investigations, on and off property in question, of offenses that may have been committed against property owned or occupied by the Federal Government or persons on the property; and
- (F) carry out such other activities for the promotion of homeland security as the Secretary may prescribe.[335]

In 2009, Congress passed a law transferring FPS yet again, this time to the National Protection and Programs Directorate (NPPD).[336] It was believed that this move would enhance NPPD's role in protecting infrastructure, and that it would be a natural fit for FPS due to their role in the GFS.[337] However, this decision moved FPS out of a DHS operational law enforcement component and into a component with no law enforcement authority.[338]

D. FPS ORGANIZATION

Currently, FPS provides security and law enforcement services to over 9,000 facilities that are leased or owned by the government in the United States.[339] While FPS is a small agency in terms of numbers (with about 1,100 employees), their footprint is large with many mission areas.[340] As such, only areas that expect to play a role in establishing FPS' capacity to secure federal facility BAS networks are included in this organizational review.

---

[335] *Homeland Security Act of 2002*.

[336] Pub. L. No. 111-83, 123 Stat. 2142, 2156-57 (2009).

[337] Shawn Reese, *The Federal Protective Service and Contract Security Guards: A Statutory History and Current Status* (CRS Report No. RS22706) (Washington, DC: Congressional Research Service, 2009,. https://www.fas.org/sgp/crs/misc/RS22706.pdf.

[338] Ibid.

[339] "The Federal Protective Service," U.S. Department of Homeland Security.

[340] Ibid.

FPS is geographically organized into three zones, each lead by a member of the Senior Executive Service. These three zones are responsible for 11 geographic regions, which are further decentralized by districts and areas, and supported by a national headquarters.[341] Within each region are three branches: a threat mitigation branch, which is responsible for criminal investigations, intelligence, federal facility covert security testing, and contract suitability investigations; a risk management branch, responsible for managing the regional contract guard program and the technical countermeasures program; and a mission support branch, responsible for providing administrative and logistical support services. FPS districts and areas are established based on locations of FPS protected facilities; they provide law enforcement and security services, conduct facility security assessments, and oversee FPS contract protective security officers (PSOs).[342]

1. Mission Support

FPS mission support operations are supported by 12 mission support functions, which are aligned with NPPD's lines of business functions.[343] The FPS mission support functions are:

1. Human Capital
2. Budget, Finance, Revenue, and Performance Management
3. Acquisition Management
4. Procurement
5. Information Technology
6. Logistics, Facilities, Fleet, and Property Accountability and Management
7. Policy and Contingency Planning
8. Public Affairs
9. Personnel Security

---

[341] Federal Protective Service, *Mission Paper* (Washington, DC: U.S. Department of Homeland Security, 2012), 16–17.

[342] Ibid., 18.

[343] Ibid.

10. Office of General Counsel

11. Labor Relations

12. Executive Secretariat[344]

There are many challenges in creating a cybersecurity capability within FPS including recruitment and training. During a March 2013 hearing before the House of Representatives, then-FBI Director Mueller stated that the cyber threat would surpass the terrorism threat to America in the coming years, perhaps due in large part to a lack of cybersecurity specialists with the knowledge, skills, and abilities needed to confront potential adversaries.[345] The lack of cybersecurity specialists is most severe in the federal government; the shortage undermines the nation's cybersecurity and remains a challenge for any future FPS cybersecurity initiative.[346]

2. EPS Funding Structure

FPS is unique in its funding structure, as it not funded by yearly congressional appropriations.[347] All FPS expenses must be funded by revenue received from two sources: a "basic security fee" paid by federal facility tenants and reimbursable and building-specific revenues that amount to 74 cents per square foot for all FPS-protected GSA-controlled space.[348] In essence, "All of FPS's security fees are available to FPS, without fiscal year limitation, for necessary expenses related to the protection of federally owned and leased buildings for FPS operations."[349] The square footage in the GSA

---

[344] Federal Protective Service, *Mission Paper*.

[345] House of Representatives Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, *Government Printing Office*, March 13, 2013. http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg79878/html/CHRG-113hhrg79878.htm; Tom Gjelten, "Cyberwarrior Shortage Threatens U.S. Security," National Public Radio, July 19, 2010, http://www.npr.org/templates/story/story.php?storyId=128574055.

[346] Amanda Vicinanzo, "Cyber Professional Shortage Likely To Solve Itself, RAND Study Finds," *Homeland Security Today*, June 20, 2014, http://www.hstoday.us/briefings/industry-news/single-article/cyber-professional-shortage-likely-to-solve-itself-rand-study-finds/516c27ccca94c0b5d8744301d332a3f3.html.

[347] U.S. Government Accountability Office, *Budget Issues: Better Fee Design Would Improve Federal Protective Service's and Federal Agencies' Planning and Budgeting for Security* (GAO-11-492) (Washington, DC: U.S. Government Accountability Office, 2011), 5.

[348] Federal Protective Service, *Mission Paper*, 51.

[349] U.S. Government Accountability Office, *Budget Issues*, 5.

inventory varies due to changes in facility occupancy; however, the average revenue collected in 2012 was approximately $270.1 million.[350] Generally, before FPS can take part in an activity, FPS must ensure the activity aligns with this funding allocation by contributing to protecting federal government property; this ensures that "1) There is a permissible funding source; 2) There is separate reimbursement for duties that otherwise fall within FPS law enforcement authority but are not funded; or 3) There is some other legal authority to conduct the activity in the absence of reimbursement."[351]

3. Training and Professional Development

FPS training and professional development (TPD) is led by a member of the SES, and assists the FPS in accomplishing its mission to protect federal facilities and those who occupy them. FPS TPD is aligned with FPS strategic goals, including "sustainment of a valued, highly skilled, and agile law enforcement, security, and mission support workforce."[352]FPS TPD has established 11 core training functions that allow it to "assess, mitigate, and respond to current and emerging threats to federal facilities."[353] The 11 core training functions are:

1. Entry-Level Training
2. Special Skills Training
3. In-Service Certifications
4. Career and Professional Development
5. Field Training Program Management
6. Advanced, Technical and Refresher Training
7. Mission Support Training
8. PSO Training
9. FPS Officer Safety Training

---

[350]U.S. Government Accountability Office, *Budget Issues*, 5.

[351] Federal Protective Service, *Mission Paper*, 2–3.

[352] Ibid., 42

[353] Ibid., 42.

10. Training Exercises

11. FPS Lessons Learned[354]

TPD does have the infrastructure in place to support cyber risk assessment training for FPS employees, and for subsequent criminal investigations into intrusions. Almost every aspect of this endeavor, however, would need to be conducted by organizations outside of FPS, as FPS does not have expertise in either subject area. However, ICS-CERT, also housed in NPPD, is uniquely situated to provide some training to FPS on BAS network security assessment methods, as well as training on the NPPD-developed assessment tool, CSET. Additionally, FPS could utilize the National Cybersecurity Workforce Framework issued by the DHS National Initiative for Cybersecurity Education (NICE).[355] The framework categorizes various cybersecurity-related functions, from vulnerability assessment and management to criminal investigations and software acquisition, and offers necessary knowledge, skills, and abilities associated with each task.[356]

NICE, administered by US-CERT, also has a training portal on its website where federal employees or nonfederal civilians can search for cybersecurity-related training classes.[357] Several of the training programs located on the NICE portal include entry-level training programs available at the Federal Law Enforcement Training Center and the Defense Cyber Investigative Training Academy; these programs could equip FPS with a strong foundation in computer and network forensics.[358] Once entry-level courses are completed, FPS employees would be prepared for more advanced training in network and control system forensics from such notable institutions as SANS and the Carnegie

---

354 Federal Protective Service, *Mission Paper*, 43–48.

355 "DRAFT National Cybersecurity Workforce Framework Version 2.0," National Initiative for Cybersecurity Careers and Studies, accessed June 20, 2015, http://niccs.us-cert.gov/research/draft-national-cybersecurity-workforce-framework-version-20.

356 Ibid.

357 "Education and Training Catalog Search," National Initiative for Cybersecurity Careers and Studies, accessed June 20, 2015, http://niccs.us-cert.gov/training/tc/search.

358 "Training Catalog," Federal Law Enforcement Training Center, accessed June 20, 2015, https://www.fletc.gov/training-catalog; "Course Homepage," Defense Cyber Investigative Training Academy, accessed June 20, 2015, https://www.dcita.edu/courses.html.

Mellon Institute, touted by DOD cybersecurity experts.[359] Successful completion of advanced training courses is necessary to conduct forensically sound investigations into such technically demanding areas as BAS facility network intrusions.[360]

E. ANALYSIS AGAINST EVALUATION CRITERIA

As mentioned in Chapter III, each option is analyzed using five evaluation criteria.[361] Table 3 summarizes the assessment of Option III against these criteria.[362]

Table 3. Option III Evaluation

Option	DHS Acceptability	Compliance	Implementation	Effectiveness	Time
III	Medium	Partially Compliant	Very Difficult	Medium	Major

(1) DHS Acceptability

The acceptability rating for Option III is assessed as medium due to the time it would take FPS to establish a viable cybersecurity program.[363] Although FPS leadership is expected to embrace at least part of Option III—namely, the inclusion of a cyber-component to the existing FPS FSA process—they may be less enthusiastic about the expense and time associated with hiring new personnel and training new or existing personnel for this new mission.

However, Option III offers the potential for several benefits for FPS. If FPS becomes proficient in BAS network intrusion investigations, it is possible FPS could expand their cyber role to assist tenant agencies with network intrusion investigations.

---

[359] Gregory Conti, James Caroland, Thomas Cook, and Howard Taylor, "Self-Development for Cyber Warriors," *Small WarsJournal*, November 10, 2011, http://smallwarsjournal.com/sites/default/files/893-conti.pdf.

[360] Ibid.

[361] Consolini, "Regional Security Assessments."

[362] Ibid.

[363] Ibid.

This new mission could possibly be funded with a direct appropriation or reimbursed directly from the agency FPS is assisting. Knowing FPS is actively engaged in successfully combating emerging threats could have a long-lasting, positive impact on the FPS-federal facility tenant relationship. Option III would also create a professional development opportunity for special agents currently hampered by nonexistent career tracks.

(2) Compliance with Laws, Presidential Executive Orders, and Directives

Option III is partially compliant with FISMA because it provides a plan to secure the physical and technical assets that support U.S. critical infrastructure.[364] It is compliant with the NCPA because it provides for a cyber-incident response plan. Option III has the potential to be partially compliant with HSPD-23 because EINSTEIN may be protecting federal facility BAS deployed on the GSA network (not, however, those housed on contractor-owned networks). Further, the option is compliant with PPD-21 because it provides cyber incident response coordinated through ICS-CERT, and compliant with Title 18 Section 1030, which authorizes FPS to conduct criminal investigations into cyber intrusions of federal facility BAS networks.

(3) Implementation

Implementation of Option III is assessed as very difficult; the option would require creating new position descriptions, hiring additional personnel, obtaining extensive training, and creating new policies.[365] Although many federal agencies have developed internal cybersecurity educational programs and partnerships with colleges and universities to increase the size and capabilities of their cybersecurity cadres, these programs have been created to cultivate employees' skills over several (5 to 10) years, leaving the United States vulnerable in the interim.[366] It is unlikely FPS could benefit

[364] Consolini, "Regional Security Assessments."

[365] Ibid.

[366] Martin C. Libicki, Julia Pollak, David Senty, *Hackers Wanted-An Examination of the Cybersecurity labor Market,* (Santa Monica, CA: RAND, 2014), http://www.rand.org/pubs/research_reports/RR430.html.

from programs with such lengthy developmental timeframes due to the current vulnerabilities and threats federal facility BAS networks face.

According to a 2013 study conducted by the International Internet System Security Certification Consortium, 61 percent of U.S. federal agencies surveyed stated that cyber security positions are going unfilled, despite the motivation and budget to fill them.[367] The positions in most demand are for the top one percent of the best hackers available.[368] A November 2010 report (prepared by the Center for Strategic and International Studies for the President of the United States) revealed there were approximately 1,000 cybersecurity practitioners in the United States who had the skills needed to combat the cyber threat; however, the nation needs between 10,000 and 30,000 cyber warriors.[369] If FPS does create a cybersecurity program, the agency would likely be competing for the same talent with such national security-focused agencies as the CIA, FBI, and NSA. While the federal salaries these national security agencies could offer new hires would probably be comparable to FPS, it is unlikely the FPS mission of securing federal facility BAS would compare to the appeal of national security agencies' missions.

(4) Effectiveness

Option III is assessed as having a medium level of effectiveness in terms of risk reduction.[370] By incorporating a strategy that involves reoccurring risk assessment and incident response, as well as investigative follow-up of federal facility network intrusions, DHS is fulfilling its obligation to protect the cyber networks of its critical infrastructure. However, this strategy would only affect roughly a quarter of the facilities owned by the GSA, and none of the commercial facilities the GSA leases from the CFS. Additionally, because of the time and expense associated with Option III, FPS must take

[367] W. Hord Tipton, "Recommendations on Solving the U.S. Government Cyber Workforce's Acute Skills Gap," International Internet System Security Certification Consortium, December 2, 2013, https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Community/Government/10th%20Anniv%20GAB%20Recommendations%20Letter.pdf.

[368] Ibid.

[369] Karen Evans and Frank Reeder, *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters* (Washington, DC: Center for Strategic & International Studies, 2010), http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf.

[370] Consolini, "Regional Security Assessments."

into consideration retention challenges it may face; the expensive training they provide will equip employees with highly marketable skills, making them attractive to private sector employers.

(5) Time

Option III is assessed as having a major time investment due to security clearance and training requirements that would need to be met.[371] The recruitment of additional personnel is expected to take over a year but less than two. Training associated with this new mission is expected to take less than a year for experienced cybersecurity professionals, but more than two for existing FPS personnel with no cybersecurity experience.

F. OVERALL ASSESSMENT

Option III would provide DHS with an alternative long-term solution to the status quo to mitigate a significant vulnerability to federal facilitates. As the lead sector specific agency for the GFS, FPS has the statutory authority to develop a cybersecurity program; as such, Option III is assessed to be generally accepted by the DHS headquarters leadership and could be fully implemented in less than three years. While Option III cannot secure all federal facility BAS networks at this time, it provides a clear strategy to secure those currently under government control.

[371] Consolini, "Regional Security Assessments."

VI. OPTION IV: HYBRID APPROACH

Option IV consists of two sub-options; IV(A) and IV(B). Both options suggest utilizing cybersecurity contractors and the Secret Service; Option IV(A), however, only utilizes these resources until the FPS can establish a viable cybersecurity program of its own. Option IV(B) removes the FPS from the eventual operational role analyzed in Option IV(A).

A. OPTION IV(A): TEMPORARILY UTILIZING CYBERSECURITY CONTRACTORS AND THE SECRET SERVICE

Option IV(A) recommends FPS leverage its existing knowledge of federal contracts (gained through managing several contract security guard programs over many years) to immediately deploy cybersecurity contractors to begin protecting federal facility BAS. These contractors would remain until FPS could fully establish their cybersecurity program, mentioned in Chapter V. This option would immediately reduce the current identified federal facility BAS network vulnerabilities, but a lack of cybersecurity contracting expertise could create additional problems for FPS.

Additionally, Option IV(A) recommends that FPS leverage the Secret Service's incident response and cyber intrusion investigative experience, highlighted in Chapter IV, until the FPS cybersecurity program is fully operational. This recommendation provides an immediate solution to current BAS network vulnerabilities. Option IV(A) also provides FPS with a knowledge base for intrusion response and investigatory responsibilities as they are transferred from the USSS to FPS.

1. The Benefits of a Contractor-Based Approach

Due to the challenges FPS faces with establishing a credible cybersecurity program—specifically, the bureaucracy associated with hiring federal employees and the length of time needed to train its existing workforce—hiring contractors to perform BAS network assessments and provide incident response could be the answer. Burning Glass, a workforce technology firm, concluded in 2013 that it can take 36 percent longer to fill

cybersecurity vacancies than all other job postings.[372] Once FPS has established their cybersecurity program, they would take over all responsibilities previously held by the contractors they were overseeing. Additionally, these contractors could serve as experienced mentors to FPS federal personnel during the transition to an all-federal force.

As mentioned in Chapter V, the government faces an incredible challenge to hire cybersecurity professionals, despite having the motivation and budgets to do so. Lower pay, complex hiring rules, lack of independence, and intrusive background investigations have all been cited as reasons the government is having a hard time recruiting cybersecurity professionals.[373] For more than two decades, the federal government has overcome the difficulty associated with hiring extremely skilled workers by outsourcing their work to private contractors.[374] Contractors, however, can offer market prices to skilled workers who can provide qualified personnel not available within the government.[375] According to Booz Allen Hamilton, private contractors make up the majority of DHS cybersecurity workers.[376] In fact, a DHS Office of Inspector General report from 2008 found that 83 percent of the DHS Chief Information Officer's personnel were contractors.[377]

Another added benefit FPS would obtain from initially using cybersecurity contractors instead of government employees is the immediacy of the resource. Cybersecurity contractors typically already possess the skills and security clearances required to secure networks.[378] Perhaps the most convincing argument, however, is that

---

372 "Cybersecurity Jobs, 2015" Burning Glass, accessed June 20, 2015, http://www.burning-glass.com/research/cybersecurity/.

373 "Government Cyber Security Careers," Cyber Degrees, accessed June 20, 2015, http://www.cyberdegrees.org/resources/government-cyber-security-careers/.

374 Libicki, Pollak, and Senty, *Hackers Wanted*, 9.

375 Ibid.

376 Partnership for Public Service, *Cyber In-Security: Strengthening the Federal Cybersecurity Workforce* (Herndon, VA: Booz Allen Hamilton, 2009), 2, http://www.boozallen.com/media/file/CyberIn-Security_2009.pdf.

377 Office of the Inspector General, *Progress Made in Strengthening DHS Information Technology Management, but Challenges Remain* (OIG-08-91) (Washington, DC: U.S. Department of Homeland Security, 2008), https://www.oig.dhs.gov/assets/Mgmt/OIG_08-91_Sep08.pdf.

378 Libicki, Pollak, and Senty, *Hackers Wanted*, 1.

DHS is already using them. A 2012 Homeland Security Advisory Council report submitted by the Cyber Skills Task Force stated that DHS has used cybersecurity contractors to fill such jobs as security engineers, reverse engineers, and penetration testers.[379] The taskforce determined, "Contractors with the right skill mix will enable DHS to upgrade its capabilities quickly."[380] The report concluded that these same contractors may decide to later join DHS as federal employees once they "get a taste" for the DHS mission.[381]

2. Limitations of a Contractor-Based Approach

Employing private contractors is not without its challenges. For example, the contracts must be managed by federal employees, who must "establish requirements, evaluate proposals, and select contractors."[382] If the federal employee charged with oversight does not have technical knowledge to adequately administer the contract, the government could overspend for the service.[383] This knowledge gap could also cause the government to purchase unnecessary or incorrect services from the contractor.[384]

3. Leveraging the Secret Service

As stated in Chapter IV, the USSS already possesses the manpower, training, equipment, expertise, and authority to conduct criminal investigations into BAS intrusions. By leveraging USSS capabilities, FPS can take the necessary time to establish their own program. Once the FPS program is established, the USSS would be available for consultation as subject-matter experts. DHS components and subcomponent agencies already rely on one another to supplement their existing services in times of crisis. Most notably is the Secret Service's use of outside federal agents to supplement its existing

---

[379] Homeland Security Advisory Council, *Cyber Skills Task Force Report: Fall 2012* (Washington, DC: U.S. Department of Homeland Security, 2012), 5, http://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf.

[380] Ibid., 23.

[381] Ibid.

[382] Libicki, Pollak, and Senty, *Hackers Wanted*, 9.

[383] Ibid.

[384] Partnership for Public Service, *Cyber In-Security*.

security workforce during presidential campaigns.[385] Another example is the Federal Air Marshal Service, which, during times of increased threats, have relied on other federal agents within DHS to supplement its force.[386]

4. Analysis against Evaluation Criteria

Table 4 outlines the assessment of Option IV(A) against the evaluation categories.

Table 4. Option IV(A) Evaluation

Option	DHS Acceptability	Compliance	Implementation	Effectiveness	Time
IV(A)	High	Partially Compliant	Simple	Medium	Minimal

(1) DHS Acceptability

The acceptability rating for Option IV(A) is judged as high because DHS is already successfully using cybersecurity contractors on a grand scale.[387] After working as a contractor, it is believed that the contractor would have a better understanding of DHS' mission and would therefore be more likely to join DHS as a federal employee.[388] Finally, the FPS would most likely endorse this option because it allows them to fulfill their core mission of protecting federal facilities and employees almost immediately, while at the same time providing them time to eventually take over the cybersecurity mission completely.

---

[385] John King, "Presidential Campaign Puts Strain on Secret Service," CNN, June 23, 2007, http://www.cnn.com/2007/POLITICS/06/23/secret.service.strain/index.html?eref=yahoo.

[386] U.S. Government Accountability Office, *Aviation Security: Protecting Federal Air Marshal Service Could Benefit from Improved Planning and Controls* (GAO-6-203) (Washington, DC: U.S. Government Accountability Office, 2006), 8–9.

[387] Ibid.

[388] Homeland Security Advisory Council. *Cyber Skills Task Force Report*, 23.

(2) Compliance with Existing Laws, Presidential Executive Orders, and Directives

Option IV(A) is compliant with FISMA because it provides a plan to secure the physical and technical assets that support U.S. critical infrastructure. It is compliant with the NCPA because it provides for a cyber-incident response plan. Option IV(A) may be partially compliant with HSPD-23 because EINSTEIN may be protecting federal facility BAS deployed on the GSA network, not those housed on contractor-owned networks. Option IV(A) is compliant with PPD-21 because it provides cyber incident response coordinated through DHS-contracted cybersecurity professional and the USSS. Further, the option is compliant with Title 18 Section 1030, which authorizes the USSS to conduct criminal investigations into cyber intrusions of federal facility BAS networks.

(3) Implementation

Implementation of Option IV (A) is judged as simple due to the immediacy contractors and Secret Service Agents could begin working.[389] Although FPS would need to quickly educate its contracting officers on cybersecurity contracting issues to reduce errors or minimize errors, they could leverage existing knowledge in this area possessed by others in the DHS such as the CIO. While policies would need to be created, several cybersecurity policies governing cybersecurity contractors likely exist as evident by the proliferation of cybersecurity contractors within DHS.

(4) Effectiveness

Option IV(A) is judged as reducing risk at the medium level. By incorporating a strategy that involves reoccurring risk assessment and incident response, as well as investigative follow-up of federal facility network intrusions, the DHS is fulfilling its obligation to protect the cyber networks of critical infrastructure. However, this strategy would only affect roughly a quarter of the facilities owned by GSA and none of the commercial facilities GSA leases from the CFS.

[389] Consolini, "Regional Security Assessments."

(5) Time

Option IV(A) is judged as having a minimal time commitment due to the deployment of cybersecurity contractors almost immediately. Additionally, as cited in chapter IV, the USSS already possess the knowledge, skills, abilities and equipment to conduct cyber intrusion investigations into federal facility BAS network.

5. Overall Assessment

Option IV(A) provides the DHS with an immediate solution to a serious vulnerability. This recommendation is expected to be widely supported by the DHS, implemented quickly and fairly easily. Although the option does not secure all federal facility BAS, it does improve security for the systems that are housed on the GSA network, protected behind their firewall. This option also allows the FPS to maintain operational control of the core mission; to protect federal facilities and the people in them.

B. OPTION IV(B): PERMANENTLY UTILIZING CYBERSECURITY CONTRACTORS AND THE SECRET SERVICE

Option IV(B) is very similar to IV(A) in terms of initial contractor and USSS involvement; however, Option IV(B) removes the FPS from the eventual operational role analyzed in Option IV(A). Option IV(B) recommends FPS continue to manage cybersecurity contractors performing risk assessment and network analysis and leverage the cyber intrusion investigation experience of the USSS indefinitely.

Option IV(B) recommends FPS use contractors and the USSS to perform cybersecurity functions and investigations, as analyzed in Option IV(A). Option IV(B) recommends that FPS involvement in federal facility cybersecurity be limited to contract oversight responsibilities, much like those currently performed for the 15,000 PSOs that work in FPS-protected facilities. This option allows FPS to address the concerns raised by GAO report 15–6 in December of 2014, while also allowing them to focus on physical risk assessments to enhance the security at GSA-owned and leased facilities.

Option IV(B) also recommends FPS work with its cybersecurity contractors to provide a cyber-physical facility security assessment, which would replace the existing facility security assessment. This decision allows FPS to incorporate both cyber and physical vulnerabilities in FPS-produced vulnerability assessments, and provide mitigation recommendations to federal facility tenants.

Option IV(B) also eliminates the need for lengthy cybersecurity training for its existing employees and removes the cumbersome process associated with federal hiring. However, by deferring what some employees may view as their core mission to contractors and other law enforcement agencies, morale at FPS would likely be diminished.

1. Analysis against Evaluation Criteria

Table 5 summarizes the assessment of Option IVB against the analysis categories.[390]

Table 5. Option IV(B) Evaluation

Option	DHS Acceptability	Compliance	Implementation	Effectiveness	Time
IV(B)	Low	Partially Compliant	Simple	Medium	Minimal

(1) DHS Acceptability

The acceptability rating for Option IV(B) is judged as low, despite the anticipated acceptance at DHS headquarters.[391] It is likely that Option IV(B) would significantly affect morale among the FPS workforce due to the transfer of duties (risk assessments/criminal investigations) to outside entities. However, FPS management may be accepting of Option IV(B) because FPS still retains control over the proposed (cyber-physical facility security assessment) process. Furthermore, the author could find no

[390] Consolini, "Regional Security Assessments."

[391] Ibid.

congressional hearing, GAO, CRS, or DHS-OIG report that identified FPS criminal investigations as an area of concern; conversely, the FSA process and FPS' management of their contract guard program has been the focus of many inquiries.

(2) Compliance with Laws, Presidential Executive Orders, and Directives

Option IV(B) is compliant with FISMA because it provides a plan to secure the physical and technical assets that support U.S. critical infrastructure. It is compliant with the NCPA because it provides for a cyber-incident response plan. Option IV(B) may be partially compliant with HSPD-23 because EINSTEIN may be protecting federal facility BAS deployed on the GSA network, but not those housed on contractor-owned networks. Option IV(B) is compliant with PPD-21 because it provides cyber incident response coordinated through the DHS-contracted cybersecurity professionals and the USSS. Option IV(B) is assessed to be compliant with Title 18 Section 1030, which authorizes the USSS to conduct criminal investigations into cyber intrusions of federal facility BAS networks.

(3) Implementation

Implementation of Option IV(B) is judged as simple due to the immediacy with which contractors and Secret Service Agents could begin working.[392] Although FPS would need to quickly educate their contracting officers on cybersecurity contracting issues to minimize potential errors, they could leverage existing knowledge in this area possessed by others in DHS, such as those resident in the CIO. While policies would need to be created, several policies governing cybersecurity contractors likely exist, evidenced by the proliferation of cybersecurity contractors within DHS.

(4) Effectiveness

Option IV(B) has a medium level of risk reduction.[393] By incorporating a strategy that involves reoccurring risk assessment and incident response, as well as investigative follow-up of federal facility network intrusions, DHS is fulfilling its obligation to protect

[392] Consolini, "Regional Security Assessments."

[393] Ibid.

the cyber networks of critical infrastructure. Additionally, by incorporating a cybersecurity vulnerability assessment as a companion piece to the FPS-produced FSA, FPS is fulfilling its duties to protect federal facilities. However, this strategy would only affect roughly a quarter of the facilities owned by GSA and none of the commercial facilities the GSA leases from the CFS.

(5) Time

Option IV(B) is judged as having a minimal time commitment, as it deploys cybersecurity contractors almost immediately.[394] Additionally, as cited in Chapter IV, the USSS already possess the knowledge, skills, abilities, and equipment to conduct cyber intrusion investigations into federal facility BAS networks. Further, of the option eliminates time needed to develop an FPS cybersecurity program.

2. Overall Assessment

Option IV(B) provides DHS with an immediate, scalable solution to a serious vulnerability. This recommendation is expected to be widely supported by DHS, but not within the FPS workforce. Option IV(B) can be implemented quickly and fairly easily. Although the option does not secure all federal facility BAS, it does enhance security for those systems housed on the GSA network, protected behind their firewall. This option also allows the FPS to maintain control of the contractors by performing assessments and subsequently incorporating contractor-produced cybersecurity assessments within the FPS produced FSA as a companion piece.

[394] Consolini, "Regional Security Assessments."

THIS PAGE INTENTIONALLY LEFT BLANK

VII. COMPARATIVE ANALYSIS, POLICY RECOMMENDATIONS, CONCLUSIONS, AND FUTURE EFFORTS

This chapter offers a comparative analysis of the five options given throughout the thesis, judges the findings, and makes recommendations.[395] The analysis attempts to answer the following primary research question:

- How can DHS leverage existing federal laws, presidential directives, executive orders, and frameworks, and its current cyber and investigative capabilities to establish a strategy to secure federal facility building-automation system networks?

The following secondary research questions were also examined:

- If existing resources are not sufficient, what additional resources should be obtained to mitigate the risks?
- How should DHS leverage its components' law enforcement authorities to augment technical cyber defense measures?

The conclusion identifies the option DHS should use to leverage its existing capabilities to secure federal facility BAS, and describes the necessary employment efforts.

A. COMPARATIVE ANALYSIS AND RESULTS

In Chapters II–VI, evaluation criteria were used to assess each policy option individually, without comparing the options against each other. The results of the analysis are included in Table 6. A new option, named "Preferred Option," was included in the table and assigned ratings consistent with a hypothetical "best choice," and used to compare the five evaluated options.[396]

[395] Consolini, "Regional Security Assessments."

[396] Ibid.

Table 6. Comparative Option Evaluation

OPTION	DHS Acceptability	Compliance	Implementation	Effectiveness	Time
I	low	Not compliant	Simple	Low	Minimal
II	Medium	Partially Compliant	Somewhat Difficult	Medium	Minor
III	Medium	Partially Compliant	Very Difficult	Medium	Major
IV(A)	High	Partially Compliant	Simple	Medium	Minimal
IV(B)	Low	Partially Compliant	Simple	Medium	Minimal
Preferred Option	High	Compliant	Simple	High	Minimal

Because no policy options obtained the ratings of the preferred option, additional analysis was performed to determine which option most closely aligned with the attributes of the preferred option.

Option I (status quo) is the least preferable option, as it achieved the lowest ratings in arguably the three important implementation criteria: effectiveness, acceptability, and compliance.

Option II (leveraging existing capabilities) is an acceptable option, but not the preferred one. The time investment associated with recruiting new hires, while reasonable, would delay the implementation of a strategy to secure federal facility BAS for at least a year.

Option III (establishing a cybersecurity program in FPS) is unacceptable by itself. The level of difficulty and the major time investments associated with developing a cybersecurity program form the ground up cannot solve the current cybersecurity vulnerabilities in federal facilities in a timely manner.

Option IV(A) (hybrid temporary contractor approach), is the preferred option. Option IV(A) can be easily implemented in less than six months and allows for a high level of institutional acceptance throughout DHS components.

Option IV(B) (hybrid permanent contractor approach) is an acceptable option, but not preferred. Despite a time-effective and easily implemented strategy, Option IV(B) eliminates the opportunity for FPS law enforcement personnel to be directly involved in the strategy.

Although Option IV(A) is the most preferred option, it is still not fully compliant with all laws, E.O.s and directives, as it does not secure the federal facility BAS networks controlled by the private contractors who maintain the networks. Once the remaining federal facility BAS networks are moved to the GSA network and protected behind the GSA firewall, Option IV(A) would attain the highest possible rating for each of the five assessment criteria.

B. CONCLUSION

Security of federal facilities has evolved greatly since the Oklahoma City bombing in 1995. While physical security vulnerabilities have remained a concern for federal facilities in the intervening years, cybersecurity has also emerged as a significant vulnerability that must be addressed sooner rather than later. The GSA's efforts to modernize their facilities and improve energy efficiency (through Internet-based BAS) have also made these facilities vulnerable to a cyber-attack. The consequences of a successful attack could range from loss of productivity to loss of life. A recurring theme throughout this thesis is that neither DHS nor the GSA has control over all GSA-owned federal facility BAS networks. The majority of these networks are controlled by a private contractor, and DHS has no visibility into these networks' cybersecurity measures.

This thesis has shown that federal facility BAS networks are vulnerable to exploitation and, despite current federal laws mandating they be secured, they remain remarkably unsecure. DHS has the legal authority and capabilities to protect these networks, but neither has yet been leveraged. This thesis offered five policy options for DHS leadership to consider as the Department moves forward with their stated goal of securing federal facility BAS networks. Each option was weighed against several evaluative criteria to include: DHS acceptability, compliance with existing laws, , implementation, effectiveness, and time.

The comparative analysis findings demonstrated that DHS should embrace and implement Option IV(A) by initially utilizing experienced, cleared private contractors to perform risk assessments and network analysis of federal facility BAS. Additionally, Option IV(A) calls for the USSS to provide incident response to network intrusions, as well as subsequent criminal investigations into the discovered intrusions. The USSS is the only DHS law enforcement component with both the authority and the technical expertise to take on this mission, gained through their work on the Critical Systems Protection Program. It is assessed that Option IV(A) will provide the necessary protection for federal facility BAS networks until FPS is able to develop and deploy their own cybersecurity program. This option provides an almost immediate, cost-effective risk mitigation strategy to reduce the vulnerabilities identified in GAO report 15–6.

C. FUTURE EFFORTS

DHS should address two areas of concern if they intend to adopt the recommended policy option offered in this thesis. Although the areas of concern will not prevent the option's implementation, overcoming them early will increase the chances for success.

First, DHS should request the Office of Management and Budget increase the basic security fee dollar amount that FPS collects to account for the additional services FPS will be providing federal facility tenants in the form of cybersecurity. If this is not viable, DHS should lobby Congress on behalf of FPS to obtain direct appropriations related to the new FPS capability.

Second, DHS must contend with the lack of government visibility on those federal facility BAS networks currently out of the government's control. DHS should establish a dialogue with the GSA to identify if existing contracts between GSA and the private contractors that maintain the majority of the BAS networks can be modified to allow for their security.

LIST OF REFERENCES

Begg, Christopher, and Matthew Warren. "Safeguarding Australia from Cyber-terrorism: A SCADA Risk Framework." In *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions*, edited by John Walp, Manish Gupta, and Raj Sharman: 369–84. Hershey, PA: IGI Global, 2012. doi: 10.4018/978-1-4666-0197-0.ch021.

Bridges, Antony. "Industrial Control Systems; The Human Threat," in *Securing Critical Infrastructures and Critical Control Systems Approaches for Threat Protection*, edited by Christopher Lanig, Atta Badii, and Paul Vickers: 82–104. Hershey, PA: IGI Global, 2013. doi: 10.4018/978-1-4666-2659-1.ch004.

Brooks, David. "Security Threats and Risks of Intelligent Building Systems: Protecting Facilities From Current and Emerging Vulnerabilities." In *Securing Critical Infrastructures and Critical Control Systems Approaches for Threat Protection*, edited by Christopher Lanig, Atta Badii, and Paul Vickers: 1–16. Hershey, PA: IGI Global, 2013. doi: 10.4018/978-1-4666-2659-1.ch001.

Burning Glass. "Cybersecurity Jobs, 2015." Accessed June 20, 2015. http://www.burning-glass.com/research/cybersecurity/.

CenturyLink. "CenturyLink Awarded New DHS EINSTEIN 3 Accelerated Task Order." December 8, 2014. http://news.centurylink.com/news/centurylink-awarded-new-dhs-einstein-3-accelerated-task-order.

Chipley, Michael. "Cybersecurity: Introduction." Whole Building Design Guide. October 23, 2014. http://www.wbdg.org/resources/cybersecurity.php?r=secure_safe.

Coburn, Tom. "A Review of the Department of Homeland Security's Missions and Performance." U.S. Senate Committee on Homeland Security & Governmental Affairs. January 2015. file:///C:/Users/abhousto/Downloads/Senator%20Coburn%20DHS%20Report%20FINAL.pdf.

Consolini, Todd R. "Regional Security Assessments: A Regional Approach to Securing Federal Facilities." Master's thesis, Naval Postgraduate School, 2009.

Conti, Gregory, James Caroland, Thomas Cook, and Howard Taylor. "Self-Development for Cyber Warriors." *Small Wars Journal*. November 10, 2011. http://smallwarsjournal.com/sites/default/files/893-conti.pdf.

Cyber Degrees. "Government Cyber Security Careers." Accessed June 20, 2015. http://www.cyberdegrees.org/resources/government-cyber-security-careers/.

Defense Cyber Investigative Training Academy. “Course Homepage.” Accessed June 20, 2015. https://www.dcita.edu/courses.html.

Evans, Karen, and Frank Reeder. *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters*. Washington, DC: Center for Strategic & International Studies, 2010. http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf.

Federal Business Opportunities. “Building Automation System Upgrade.” June, 24, 2014. https://www.fbo.gov/index?s=opportunity&mode=form&id=4a0d482d88af8b5b7f35b01eb837b024&tab=core&_cview=1.

Federal Law Enforcement Training Center. “Training Catalog.” Accessed June 20, 2015. https://www.fletc.gov/training-catalog

Federal Protective Service. *Mission Paper*.(Washington, DC: U.S. Department of Homeland Security, 2012.

Fischer, Eric A. *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*. (CRS Report No. R42114). Washington, DC: Congressional Research Service. https://www.fas.org/sgp/crs/natsec/R42114.pdf.

Fisher, Dennis, and Paul Roberts. “Threat Post: Stuxnet.” Kaspersky Lab. Accessed October 21, 2015. http://usa.kaspersky.com/sites/usa.kaspersky.com/files/TP-Spotlight-Stuxnet.pdf.

General Services Administration. *Facility Standards for the Public Building Service*. (PBS-P100 2015). Washington, DC: General Services Administration, 2015. http://www.gsa.gov/portal/mediaId/225771/fileName/2015_P100_FacilitiesStandards.action.

———. “Inventory of Owned and Leased Properties.” Accessed June 13, 2015. http://www.gsa.gov/portal/content/100783.

———. “ New Smart Building Technology to Increase Federal Buildings Energy Efficiency.” May 12, 2012. http://www.gsa.gov/portal/content/135115.

Gjelten, Tom. “Cyberwarrior Shortage Threatens U.S. Security.” National Public Radio. July 19, 2010. http://www.npr.org/templates/story/story.php?storyId=128574055.

Greenberg, Andy and Kim Zetter. “Why the OPM Breach Is Such a Security and Privacy Debacle.” *Wired*. June 11, 2015.

Homeland Security Advisory Council. *Cyber Skills Task Force Report: Fall 2012*. Washington, DC: U.S. Department of Homeland Security, 2012. http://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf.

House of Representatives Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, *Government Printing Office,* March 13, 2013. http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg79878/html/CHRG-113hhrg79878.htm.

ICS-Cert Monitor, (October/November/December 2012). http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf.

Industrial Control Systems Cyber Emergency Response Team. *Control System Internet Accessibility*. (ICS-ALERT-10-301-01). Washington, DC: U.S. Department of Homeland Security. http://ics-cert.us-cert.gov/alerts/ICS-ALERT-10-301-01.

———. "CSET Homepage." June 14, 2015. https://ics-cert.us-cert.gov/sites/default/files/FactSheets/CSET%20Fact%20Sheet_20140528.pdf.

———. "Homepage." June 14, 2015. https://ics-cert.us-cert.gov/.

———. *ICS-CERT Year in Review 2012*. Washington, DC: U.S. Department of Homeland Security, 2012. https://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2012_Final.pdf.

———. *ICS-CERT Year in Review 2015*. (Washington, DC: U.S. Department of Homeland Security, 2015). https://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2014_Final.pdf.

INFOSEC Institute. "The Importance of Cyber Hygiene in Cyberspace." April 30, 2015. http://resources.infosecinstitute.com/the-importance-of-cyber-hygiene-in-cyberspace/.

Interagency Security Committee. *Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper*. (PPD-21). Washington, DC: Department of Homeland Security. http://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf.

Kerr, Paul, John Rollins, and Catherine Theohary. *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability.* (CRS Report R41524). Washington, DC: Congressional Research Service, 2010. http://assets.opencrs.com/rpts/R41524_20101209.pdf.

King, John. “Presidential Campaign Puts Strain on Secret Service.” CNN. June 23, 2007. http://www.cnn.com/2007/POLITICS/06/23/secret.service.strain/index.html?eref=yahoo.

Kuehn, Andreas, and Milton Muelller. “Securitizing Critical Infrastructure, Blurring Organizational Boundaries: The U.S. Einstein Program.” Presented at the Research Conference on Communication, Information and Internet Policy, Arlington, VA, September 29, 2013.

Libicki, Martin C., Julia Pollak, David Senty. *Hackers Wanted-An Examination of the Cybersecurity labor Market.*Santa Monica, CA: RAND, 2014. http://www.rand.org/pubs/research_reports/RR430.html.

Lowery, Edward W. “Closing the Cyber Gap: Integrating Cross-Government Cyber Capabilities to Support the DHS Cyber Security Mission.” Master’s thesis, Naval Postgraduate School, 2014.

Lyngass, Sean, “Security Experts: OPM Breach Show Einstein Isn’t Enough.” *The Business of Federal* Technology.” June 5, 2015. http://fcw.com/articles/2015/06/05/opm-einstein.aspx.

Macaulay, Tyson, and Bryan Singer. *Cybersecurity for Industrial Control Systems*. Boca Raton, FL: CRC Press, 2012.

McCarthy, Justin “Americans Losing Confidence in All Branches of U.S. Gov’t.” Gallup. June 20, 2014. http://www.gallup.com/poll/171992/americans-losing-confidence-branches-gov.aspx.

McElreath, David H., Carl J. Jensen III, Michael Wigginton Jr., Daniel Adrian Doss, Robert Nations, and Jeffrey Van Slyke. *Introduction to Homeland Security,* 2nd Edition. Boca Raton, FL: CRC Press, 2013.

McHugh, John, Alan Christie, and Julia Allen. “Defending Yourself: The Role of Intrusion Detection Systems.” 17, no. 5 (September/October 2000): 42–51. https://nps.illiad.oclc.org/illiad/illiad.dll?Action=10&Form=75&Value=144466.

Mordin, Josh, and Sandy Schadchehr. “Building Monitoring and Control Systems in GSA.” Presented at the Cybersecurity Building Control Systems Workshop, Washington, DC, March 24, 2015.

National Initiative for Cybersecurity Careers and Studies. “DRAFT National Cybersecurity Workforce Framework Version 2.0.” Accessed June 20, 2015. http://niccs.us-cert.gov/research/draft-national-cybersecurity-workforce-framework-version-20.

———. “Education and Training Catalog Search.” Accessed June 20, 2015. http://niccs.us-cert.gov/training/tc/search.

National Security Council. *Cybersecurity Policy*. (NSPD-54/HSPD-23). Washington, DC: White House, 2008. https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf.

"News of Science." *American Association for the Advancement of Science* 122, No. 3169 (September 1955), 550–555.

Office of Management and Budget. *Annual Report to Congress: Federal Information Security Management Act*. Washington, DC: Executive Office of the President, 2015. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.

Office of Inspector General. *Challenges Remain in DHS' Efforts to Secure Control Systems*. (OIG-09-95). Washington, DC: U.S. Department of Homeland Security, 2009. https://www.oig.dhs.gov/assets/Mgmt/OIG_09-95_Aug09.pdf.

———. *DHS Can Make Improvements to Secure Industrial Control Systems*. (OIG-13-39). Washington, DC: U.S. Department of Homeland Security, 2013. https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-39_Feb13.pdf.

———. *Federal Protective Service: Contract Guard Procurement and Oversight Process Challenges*. (OIG-09-51). Washington, DC: U.S. Department of Homeland Security, 2009. https://www.oig.dhs.gov/assets/Mgmt/OIG_09-51_Apr09.pdf.

———. *Progress Made in Strengthening DHS Information Technology Management, but Challenges Remain*. (OIG-08-91). Washington, DC: U.S. Department of Homeland Security, 2008. https://www.oig.dhs.gov/assets/Mgmt/OIG_08-91_Sep08.pdf.

Partnership for Public Service. *Cyber In-Security: Strengthening the Federal Cybersecurity Workforce*. Herndon, VA: Booz Allen Hamilton, 2009. http://www.boozallen.com/media/file/CyberIn-Security_2009.pdf.

Pearlson, Keri E., and Carol S. Saunders. *Managing and Using Information Systems*, 5th ed. Hoboken, NJ: John Wiley and Sons, 2013.

President of the United States. *Homeland Security Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection*. (HSPD-7). Washington, DC: U.S. Department of Homeland Security, 2003. http://www.dhs.gov/homeland-security-presidential-directive-7.

———. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: White House, 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

———. *Presidential Policy Directive—Critical Infrastructure Security and Resilience*. (PPD-21). Washington, DC: White House, 2013.

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures*. Washington, DC: White House, 1997.

Preston, Keith. *Attack the System: A new anarchist Perspective for the 21st Century*. London: Black House Publishing, 2013.

Ravindranath, Mohana. "Committee Grills DHS Official Over Einstein's Failure To Prevent OPM Attack." NextGov. June 24, 2015. http://www.nextgov.com/cybersecurity/2015/06/house-committee-grills-dhs-official-failure-einstein-cdm-prevent-opm-attack/116242/.

Reese, Shawn. *The Federal Protective Service and Contract Security Guards: A Statutory History and Current Status*. (CRS Report No. RS22706). Washington, DC: Congressional Research Service, 2009. https://www.fas.org/sgp/crs/misc/RS22706.pdf.

Reese, Shawn, and Lorraine H. Tong. *Federal Building and Facility Security*. (CRS Report No. R41138). Washington, DC: Congressional Research Service, 2010. https://www.fas.org/sgp/crs/homesec/R41138.pdf.

Rockwell, Mark. "New BPAs to Aid in Cyberdefense." FCW. August 14, 2013. http://fcw.com/articles/2013/08/14/dhs-cmaas.aspx?m=1.

Rojek, Kevin. "Current Cyber Threats: An Ever Changing Landscape." Presented at the Central Ohio Info Sec Summit, Columbus, OH, March 24, 2015.

Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. Santa Barbara, CA: Praeger, 2013.

SANS Institute. "InfoSec Reading Room." Last modified October 28, 2015. http://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525.

Shadchehr, Sandy, and Josh Mordin."Building Monitoring and Control Systems in GSA." Presented at the Cybersecurity Building Control Systems Workshop, Washington, DC, March 24, 2015.

Shea, Dana A. *Critical Infrastructure: Control Systems and the Terrorist Threat*. (CRS Report RL31534). Washington, DC: Congressional Research Service, 2003.

Social Security Administration. "Social Security Basic Facts." April 2, 2014. www.ssa.gov/news/press/basicfacts.html.

Sternstein, Aliya. “The Nation’s 24-Hour Cyber Watch Center Still Has Some Empty Seats.” NextGov. August 24, 2015. http://www.nextgov.com/cybersecurity/2015/08/nations-24-hour-hack-watch-center-missing-three-quarters-industry/119392/?oref=govexec_today_nl.

Stouffer, Keith. *NIST Briefing: ICS Cybersecurity Guidance—NIST SP 800–82, Guide to ICS Security*. Gaithersburg, MD: National Institute of Standards and Technology, 2013. http://www.businessofsecurity.com/docs/BOS_NIST%20ICS%20Briefing_Keith%20Stouffer%208-28-13.pdf.

Stouffer, Keith, Joe Falco, and Karen Scarfone. *Guide to Industrial Control Systems (ICS) Security*. (NIST Special Publication 800–82). Gaithersburg, MD: National Institute of Standards and Technology, 2011. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

Tipton, W. Hord. “Recommendations on Solving the U.S. Government Cyber Workforce’s Acute Skills Gap.” International Internet System Security Certification Consortium. December 2, 2013. https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Community/Government/10th%20Anniv%20GAB%20Recommendations%20Letter.pdf.

Tong, Lorraine H. *Federal Building and Facility Security*. (CRS Report No. R41138). Washington, DC: Congressional Research Service, 2010.

United States Marshals Service. *Vulnerability Assessment of Federal Facilities*. Washington, DC: U.S. Department of Justice, 1995. https://www.ncjrs.gov/pdffiles1/Digitization/156412NCJRS.pdf.

U.S. Department of Homeland Security. “About The National Cyber Security and Communications Integration Center,” June 16, 2015. http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

———. “CSET Frequently Asked Questions.” Accessed June 18, 2015, https://ics-cert.us-cert.gov/CSET-FAQ.

———. “The Federal Protective Service.” June 13, 2015. http://www.dhs.gov/federal-protective-service-0.

———. *National Infrastructure Protection Plan.* (NIPP 2013). Washington, DC: U.S. Department of Homeland Security, 2013. http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

———. *Strategy for Securing Control Systems: Coordinating and Guiding Federal, State, and Private Sector Initiatives*. Washington, DC: U.S. Department of Homeland Security, 2009. https://ics-cert.us-cert.gov/sites/default/files/documents/Strategy%20for%20Securing%20Control%20Systems.pdf.

U.S. Department of Justice. *Prosecuting Computer Crimes*. Washington, DC: Office of Legal Education Executive Office for United States Attorneys.

———. *Vulnerability Assessment of Federal Facilities*. Washington, DC: U.S. Department of Justice, 1995. https://www.ncjrs.gov/pdffiles1/Digitization/156412NCJRS.pdf.

U.S. General Services Administration. "Memorandum of Agreement Between the Department of Homeland Security, Office of Cybersecurity & Communications and _____." Last modified March 25, 2015. www.gsa.gov/portal/getMediaData?mediaId=169487.

———. "Trusted Internet Connections (TICS)." Last modified March 25, 2015. http://www.gsa.gov/portal/content/104213.

U.S. Government Accountability Office. *Aviation Security: Protecting Federal Air Marshal Service Could Benefit from Improved Planning and Controls*. (GAO-6-203). Washington, DC: U.S. Government Accountability Office, 2006.

———. *Budget Issues: Better Fee Design Would Improve Federal Protective Service's and Federal Agencies' Planning and Budgeting for Security*. (GAO-11-492). Washington, DC: U.S. Government Accountability Office, 2011.

———. *Building Security: Interagency Security Committee Has Had Limited Success in Fulfilling its Responsibilities*. (GAO-02-1004). Washington, DC: U.S. Government Accountability Office, 2002.

———. *Building Security: Security Responsibilities for Federally Owned and Leased Facilities*. (GAO-03-8). Washington, DC: U.S. Government Accountability Office, 2002.

———. *Critical Infrastructure Protection: Challenges in Securing Control Systems*. (GAO-04-140T). Washington, DC: U.S. Government Accountability Office, 2003. http://www.gao.gov/assets/120/110405.pdf.

———. *Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems.* (GAO-15-6). Washington, DC: U.S. Government Accountability Office, 2014. http://www.gao.gov/assets/670/667512.pdf.

———. *Federal Law Enforcement: Results of Surveys of Federal Civilian Law Enforcement Components*. (GAO-07-223SP). Washington, DC: U.S. Government Accountability Office, 2006. http://www.gao.gov/products/GAO-07-223SP.

———. *Federal Protective Service: Protecting Federal Facilities Remains a Challenge*. (GAO-14-623T). Washington, DC: U.S. Government Accountability Office, 2014.

———. *High-Risk Series: An Update*. (GAO-13-283). Washington, DC: U.S. Government Accountability Office, 2013. http://www.gao.gov/assets/660/652133.pdf.

———. *Homeland Security: Federal Protective Service's Use of Contract Guards Requires Reassessment and More Oversight*. (GAO-10-614T). Washington, DC: U.S. Government Accountability Office, 2010. http://www.gao.gov/new.items/d10614t.pdf.

———. *Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices*. (GAO-05-49). Washington, DC: U.S. Government Accountability Office, 2004.

———. *Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections At Federal Agencies*. (GAO-10-237). Washington, DC: U.S. Government Accountability Office, 2010.

———. *Information Security: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*. (GAO-15-758T). Washington, DC: U.S. Government Accountability Office, 2015. http://www.gao.gov/assets/680/671253.pdf.

———. *Multiple Efforts to Secure Control Secure Control Systems Are Under Way, but Challenges Remain.* (GAO-07-1036). Washington, DC: U.S. Government Accountability Office, 2007. http://www.gao.gov/assets/270/268137.pdf.

———. *Homeland Security: The Federal Protective Service Faces Several Challenges That Hamper its Ability to Protect Federal Facilities*. (GAO-08-683). Washington, DC: U.S. Government Accountability Office, 2008. http://www.gao.gov/new.items/d08683.pdf.

U.S. Secret Service. "National Computer Forensic Institute Homepage." Accessed June 18, 2015. https://www.ncfi.usss.gov/ncfi/pages/about.jsf;jsessionid=+vrHq3hgwno7QSmSkZ3mHtUw.

Vicinanzo, Amanda. “Cyber Professional Shortage Likely To Solve Itself, RAND Study Finds.” *Homeland Security Today*. June 20, 2014. http://www.hstoday.us/briefings/industry-news/single-article/cyber-professional-shortage-likely-to-solve-itself-rand-study-finds/516c27ccca94c0b5d8744301d332a3f3.html.

Vijayan, Jaikumar. “Target Attack Shows Danger of Remotely Accessible HVAC Systems.” Computer World. February 7, 2014. http://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html.

Weiss, N. Eric. *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis*. (CRS Report No. R43821). Washington, DC: Congressional Research Service, 2015.

Zelvin, Larry. “National Cybersecurity & Communications Integration Center (NCCIC) Overview.” Presented at the Information Security and Privacy Advisory Board, Washington, DC, October 12, 2012.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California