NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MITIGATING RISK TO DOD INFORMATION NETWORKS BY IMPROVING NETWORK SECURITY IN THIRD-PARTY INFORMATION NETWORKS

by

Michael J. Kansteiner

June 2016

Thesis Advisor: Raymond R. Buettner Jr.
Second Reader: Ramsey Meyer

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 June 2016	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE MITIGATING RISK TO DOD INFORMATION NETWORKS BY IMPROVING NETWORK SECURITY IN THIRD-PARTY INFORMATION NETWORKS	5. FUNDING NUMBERS
6. AUTHOR(S) Michael J. Kansteiner	
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)

Poorly defended third-party information networks can act as an attack vector for cyber attackers to successfully breach larger and more robustly defended information networks. Therefore, third-party networks connecting to Department of Defense (DOD) information networks may pose a significant risk to the DOD. The DOD has attempted to alleviate this risk to its networks by requiring covered defense contractors to meet certain network security standards and by initiating a cyber threat information sharing program: the DOD Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program. However, these DOD actions are not aggressive enough to adequately mitigate this risk to DOD networks. To adequately address this problem, an expanded and more aggressive incentive-based program is required. Existing federal government, incentive-based programs were analyzed as potential exemplars from which to build a new incentive-based network security program. The Department of Homeland Security's (DHS's) Safety Act Program was ultimately chosen as the primary exemplar. Using this model, an Enhanced DOD CS/IA Program was designed to offer the DOD a system that can influence the improvement of third-party network security through a structure of synchronized network security controls and incentives. By implementing the proposed DOD Enhanced CS/IA Program to improve the network security of third-party networks that connect to DOD networks, the DOD can better mitigate the risk of cyber attacks to its own networks.

14. SUBJECT TERMS network security, information networks, third-party networks, incentives, DODIN	15. NUMBER OF PAGES 139
	16. PRICE CODE

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

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MITIGATING RISK TO DOD INFORMATION NETWORKS BY IMPROVING NETWORK SECURITY IN THIRD-PARTY INFORMATION NETWORKS

Michael J. Kansteiner
Major, United States Marine Corps
B.S., United States Naval Academy, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2016

Approved by: Raymond R. Buettner Jr.
Thesis Advisor

Ramsey Meyer
Second Reader

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Poorly defended third-party information networks can act as an attack vector for cyber attackers to successfully breach larger and more robustly defended information networks. Therefore, third-party networks connecting to Department of Defense (DOD) information networks may pose a significant risk to the DOD. The DOD has attempted to alleviate this risk to its networks by requiring covered defense contractors to meet certain network security standards and by initiating a cyber threat information sharing program: the DOD Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program. However, these DOD actions are not aggressive enough to adequately mitigate this risk to DOD networks. To adequately address this problem, an expanded and more aggressive incentive-based program is required. Existing federal government, incentive-based programs were analyzed as potential exemplars from which to build a new incentive-based network security program. The Department of Homeland Security's (DHS's) Safety Act Program was ultimately chosen as the primary exemplar. Using this model, an Enhanced DOD CS/IA Program was designed to offer the DOD a system that can influence the improvement of third-party network security through a structure of synchronized network security controls and incentives. By implementing the proposed DOD Enhanced CS/IA Program to improve the network security of third-party networks that connect to DOD networks, the DOD can better mitigate the risk of cyber attacks to its own networks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- A. THIRD-PARTY NETWORK ATTACK SCENARIO....6
- B. PURPOSE....9
- C. ANALYSIS METHODS....9

II. LITERATURE REVIEW....13
- A. INTRODUCTION....13
- B. NETWORK VULNERABILITY ASSESSMENTS....13
- C. CYBER SECURITY REPORTS....16
- D. THIRD-PARTY NETWORK ATTACKS....22
- E. U.S. GOVERNMENT CYBER SECURITY ACTIONS....25
- F. FINANCIAL ASPECTS OF CYBER ATTACKS....29
- G. SYSTEMS ENGINEERING APPROACH....38
- H. CONCLUSION....44

III. EXISTING FEDERAL GOVERNMENT PROGRAMS....45
- A. INTRODUCTION....45
- B. DHS SAFETY ACT PROGRAM....45
- C. DOD DIB CS/IA PROGRAM....51
- D. ANALYSIS....53
- E. SUMMARY....54

IV. ANALYSIS OF PROPOSED MODIFICATIONS TO THE DOD DIB CS/IA PROGRAM....57
- A. OVERVIEW....57
- B. PROPOSED DOD CS/IA PROGRAM STRUCTURE....58
  - 1. The Basic Tier....59
  - 2. The Advanced Tier....63
- C. ENHANCED DOD CS/IA PROGRAM ADMINISTRATION....67
- D. THE ENHANCED PROGRAM'S ASSOCIATED COSTS....68
- E. SUMMARY....71

V. CONCLUSION AND RECOMMENDATIONS....73
- A. CONCLUSION....73
- B. RECOMMENDATIONS....76
- C. SUGGESTIONS FOR FUTURE WORK....77

APPENDIX A. CURRENT U.S. TRANSCOM CONTRACTOR DATA.....79

APPENDIX B. EXAMPLE ENHANCED DOD CS/IA PROGRAM SELF-ASSESSMENT FORM.....81

APPENDIX C. SAFETY ACT LEGISLATION TEXT.....103

LIST OF REFERENCES.....109

INITIAL DISTRIBUTION LIST.....117

LIST OF FIGURES

Figure 1. Cyber Threat Taxonomy 18

Figure 2. The Cost of Cyber Crime 31

Figure 3. Cost Framework for Cyber Crime 33

Figure 4. Activity Cost Comparison and the Use of Security Intelligence Technologies 34

Figure 5. Cost Savings When Deploying Seven Enabling Technologies 35

Figure 6. Estimated ROI for Seven Categories of Enabling Security Technologies 36

Figure 7. Multiple Systems (SOS) 39

Figure 8. Top-Down/Bottom-Up System Development Process 41

Figure 9. The System Engineering Process in the Life Cycle 42

Figure 10. System-of-Systems Integration and Interoperability Requirements 43

Figure 11. Safety Act Liability Levels 48

Figure 12. The Enhanced DOD CS/IA Program Structure 67

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Number of Successful Attacks against Organizations 4

Table 2. Description of Cyber Threat Tiers 17

Table 3. Defense Science Board's Estimated Cyber Security Investment Requirements 19

Table 4. Verizon Data Breach Investigations Report's Network Breach Category Patterns 20

Table 5. Cyber Attack Costs versus Other Illicit Activities.....30

Table 6. Safety Act Liability Protections Summary 50

Table 7. Summary of Enhanced Program Costs to DOD 69

Table 8. U.S. TRANSCOM Contract Data 79

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AntiSec	Anti-Security
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIS	Center for Internet Security
CJCS	Chairman of the Joint Chiefs of Staff
CND	Computer Network Defense
COMSEC	Communication Security
CS/IA	Cyber Security and Information Assurance
CSIS	Center for Strategic and International Studies
CUI	Controlled Unclassified Information
DAS	Defense Acquisition System
DC3	DOD Cyber Crime Center
DCISE	DIB Collaborative Information Sharing Environment
DCR	DOTMLPF-P Change Request
DFARS	Defense Acquisition Regulations Supplement
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DOD	Department of Defense
DODIN	DOD Information Network
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
DOS	Denial-of-Service
DSB	Defense Science Board
DSS	Defense Security Service
DT&E	Developmental Test & Evaluation
EDI	Electronic Data Interchange
FA	Framework Agreement
FCL	Facility Security Clearance
FAR	Federal Acquisition Regulations
FY	Fiscal Year

GDP	Gross Domestic Product
GS	General Schedule
INCOSE	International Council on Systems Engineering
IT	Information Technology
JCIDS	Joint Capabilities Integration and Development System
JKO	Joint Knowledge Online
MDD	Material Development Decision
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POS	Point-of-Sale
QATT	Qualified Anti-Terrorism Technology
ROI	Return-on-Investment
SC	Security Category
SMS	Single Mobility System
SOS	System-of-Systems
SP	Special Publication
SQL	Structured Query Language
SSI	Strategic Studies Institute
TRANSCOM	Transportation Command
UCTI	Unclassified Controlled Technical Information
UL	Underwriters Laboratories
USD AT&L	Under Secretary of Defense for Acquisition, Technology, and Logistics

EXECUTIVE SUMMARY

On July 12, 2011, Department of Defense (DOD) contractor Booz Allen Hamilton acknowledged its network had been breached by the hacktivist group Anti-Security (AntiSec).[1] Using the Booz Allen Hamilton network as an attack vector, the group gained access to the DOD's Joint Knowledge Online (JKO) portal. On September 17, 2014, the Senate Armed Services Committee released a report from an inquiry it conducted concerning information known to the U.S. Transportation Command (TRANSCOM) about cyber targeting against its contractors. The report stated that from June 01, 2012, to May 30, 2013, there were 50 successful known network intrusions against TRANSCOM contractors.[2] These examples show that third-party information networks represent a clear risk to the DOD and its operational security. The purpose of this thesis is to improve the security of the DOD Information Network (DODIN) by proposing a system that can influence improved network security in third-party networks that exchange information with the DODIN.

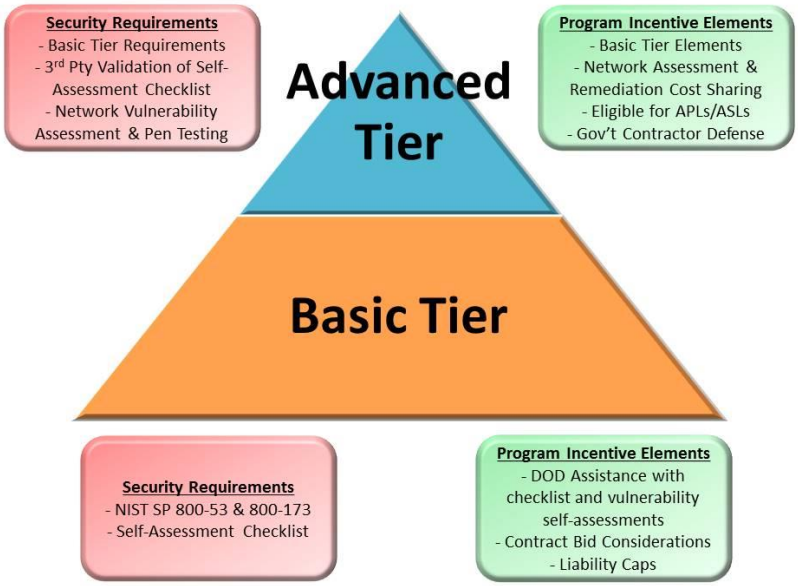
The current DOD Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program was a starting point for the DOD to reach out to and assist the private sector in improving its network security. However, the application of the current program is too narrow, and it does not have the capability to influence all third-party non-DOD networks that contact some part of the DODIN. Also, the DOD DIB CS/IA Program could do more to further incentivize improved network security of private sector third-party networks.

The DOD DIB CS/IA Program can be significantly enhanced by restructuring it into a two-tiered, incentive-based information network security program. This

1 Acunetix, "Anonymous Hack U.S. Department of Defence—Analysis of the Attack," *Acunetix Blog*, August 4, 2011, http://www.acunetix.com/blog/news/anonymous-hack-us-department-of-defence-analysis/.

2 Senate Committee on Armed Services, Inquiry in Cyber Intrusions Affecting U.S. Transportation Command Contractors, 113th Cong., i, (September 17, 2014).

restructured program is called the Enhanced DOD CS/IA Program. The enhanced program's two tiers are basic and advanced. Each tier in this program contains different levels of security requirements and incentive elements for participants. Figure 1 presents a visual depiction of the Enhanced DOD CS/IA Program including its security requirements and incentive elements:



The width of each tier represents the relative number of expected participants at that tier.

Figure 1. The Enhanced DOD CS/IA Program Structure

Another course of action for the Enhanced DOD CS/IA Program potentially exists. In this course of action, the federal government would give control of the enhanced program to the Department of Homeland Security (DHS). Several reasons exist why this course of action makes sense and should be considered. First, one of DHS's core missions is to work with the private sector to secure information networks.[3] Second, due to its mission set, DHS has the ability to expand the program's effects further because DHS can apply it to the whole of government.

3 "Our Mission," Department of Homeland Security, accessed April 8, 2016, https://www.dhs.gov/our-mission.

The author recommends the DOD implement the Enhanced DOD CS/IA Program as it is presented in this thesis. The author also recommends that the DOD and DHS begin discussions to determine which department should operate and control the enhanced program. The author recommends placing program control under DHS because dealing with the security of private sector information networks is a DHS core mission and the program will have greater ability to reduce risk to whole of government and private sector under DHS.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my wife, Sarah Kansteiner, and our boys, James and Cole, for having patience with me these past two years and especially these last few months. I know it has not always been easy seeing me here but not really “here.” Thank you for all of the support and understanding. I could not have accomplished this without you.

I would also like to thank Dr. Raymond Buettner, Mr. Ramsey Meyer, and Ms. Cheryl Huddleston for all of your advice, mentoring, and editing support. You helped to unlock my mind and get the ideas flowing. I am not sure that would have happened otherwise. Additionally, thanks must go to all the others who answered questions and provided information for this thesis. Lastly, thank you to all my fellow cohort members and classmates who have helped to get me through all the classes here at NPS and provided inspiration when I needed it.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

On December 19, 2013, the Target Corporation announced they had been the victims of an information network breach in which the credit and debit card account information of 40 million customers had been compromised.[1] Further investigation of the breach showed the attackers had been able to breach the Target network through a small business that was a third-party service provider the attackers had compromised months earlier.[2] The attackers were ultimately able to breach the Target network through a remote access billing application using the service provider's network and stolen access credentials.[3] In this case, the attackers must have assessed that the small third-party network represented a more weakly defended and more economical attack vector than any vector that directly attacked the Target Corporate network. This example demonstrates the security risk that third-party information networks pose to other networks they exchange information with. Unfortunately, many other examples of network attacks using third-party networks as attack vectors exist.

Unclassified examples of attackers using third-party networks to attack federal government networks exist but are less well known. On July 12, 2011, Department of Defense (DOD) contractor Booz Allen Hamilton acknowledged its network had been breached by the hacktivist group Anti-Security (AntiSec).[4] Using the Booz Allen Hamilton network as an attack vector, the group then used a structured query language (SQL) injection attack to gain access to the DOD's Joint Knowledge Online (JKO) portal. With that access, the group was able to download approximately 90,000 JKO user accounts containing email addresses, hashed passwords, and some personal user information.[5] Though the DOD and Booz Allen Hamilton tried to downplay the

---

[1] Senate Committee on Commerce, Science, and Transportation, A "Kill Chain" Analysis of the 2013 Target Data Breach, 113th Cong., 1, (2014).

[2] Ibid., 4.

[3] Ibid.

[4] Acunetix, "Anonymous Hack U.S. Department of Defence—Analysis of the Attack," *Acunetix Blog*, August 4, 2011, http://www.acunetix.com/blog/news/anonymous-hack-us-department-of-defence-analysis/.

[5] Ibid.

significance of the breach, analysts suggest that the attack method and the information stolen indicate that AntiSec was able to escalate its privileges within the JKO portal and penetrate deeper into the network than indicated by the victims.[6]

On September 17, 2014, the Senate Armed Services Committee released a report from an inquiry it conducted concerning information known to the U.S. Transportation Command (TRANSCOM) about cyber targeting against its contractors. The report stated that from June 01, 2012, to May 30, 2013, there were 50 successful known network intrusions against TRANSCOM contractors, with 20 of them being attributed to China.[7] The report did not specify if any TRANSCOM networks were subsequently attacked via these contractor networks, but the possibility exists that subsequent network attacks against TRANSCOM did occur. The report also states that TRANSCOM was only aware of two of the intrusions linked to China.[8] So it is also possible TRANSCOM never realized that its networks had been attacked through these contractor networks.

These examples show that third-party information networks represent a clear risk to the DOD and its operational security. In many cases, third-party networks do not maintain the same level of network security as DOD networks. Thus, attackers will likely choose to use third-party networks as a more advantageous attack vector from which to attack DOD networks. Currently, the DOD lacks an effective means to mitigate this risk, which is the problem this thesis addresses.

Examining the broader scope of cyber attacks against information networks, it is apparent they are a growing problem. They represent a common threat to the interests and capabilities of both the private sector and the DOD. Civilian network breaches at Target,[9] Home Depot,[10] and many other corporations have grabbed headlines, affected hundreds

---

[6] Ibid.

[7] Senate Committee on Armed Services, Inquiry in Cyber Intrusions Affecting U.S. Transportation Command Contractors, 113th Cong., i, (September 17, 2014).

[8] Ibid.

[9] Senate Committee on Commerce, Science, and Transportation, A "Kill Chain" Analysis of the 2013 Target Data Breach, i.

[10] Sean M. Kerner, "Home Depot Breach Expands, Privilege Escalation Flaw to Blame," *EWeek*, November 8, 2014, http://www.eweek.com/security/home-depot-breach-expands-privilege-escalation-flaw-to-blame.html.

of millions of people, and financially impacted the victim companies. The Joint Chiefs of Staff unclassified email network and the Pentagon food court network have both recently been attacked and breached.[11] Overall, cyber attacks show no sign of abating in the foreseeable future. The 2014 Verizon Data Breach Investigations Report (DBIR) recorded 63,437 cyber security incidents with 1,367 confirmed network breaches worldwide in 2013.[12] When one considers that estimates show less than 1 percent of all cyber attacks are actually reported,[13] and the contributing body to the Verizon DBIR was only 50 organizations,[14] the enormity of the threat is obvious. Data shows DOD networks alone face thousands of attacks per year.[15] Overall, evidence indicates the rate that organizations face cyber attacks is only increasing.[16] Table 1 shows successful cyber attacks against organizations participating in a Ponemon Institute research study (2015) over the past several years:

---

[11] Pierluigi Paganini, "Another Computer System at the Pentagon Has Been Hacked," *Security Affairs Blog*, September 11, 2015, http://securityaffairs.co/wordpress/40039/cyber-crime/pentagon-hacked-again.html.

[12] Verizon Enterprise, "2014 Data Breach Investigations Report," 2, (2014), http://www.verizonenterprise.com/DBIR/2014/?utm_source=earlyaccess&utm_medium=redirect&utm_campaign=DBIR.

[13] Nicholas Burns and Jonathon Price, eds., *Securing Cyberspace: A New Domain for National Security* (Queenstown, MD: Aspen Institute, February 2012), 131.

[14] Verizon Enterprise, "2014 Data Breach Investigations Report," 2.

[15] William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, September/October 2010, 97.

[16] Ponemon Institute, sponsored by Hewlett Packard, "2015 Cost of Cyber Crime Study: Global," 11 (2015). http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf.

Table 1. Number of Successful Attacks against Organizations[17]

Year	Number of Organizations	Total Number of Successful Attacks	Number of Successful Attacks per Company
2012	199	262	1.3
2013	234	343	1.4
2014	257	429	1.7
2015	252	477	1.9

The costs associated with cyber attacks can be truly staggering. A single breach at a major corporation can easily cost that company hundreds of millions of dollars or more. The Target corporation network breach current cost estimate is approximately $160 million.[18] During 2008 and 2009, the DOD reportedly spent over $100 million recovering from cyber attacks in just a six-month period.[19] Cost estimates such as those noted earlier may not even reflect the total cost of cyber attacks. Some damage from cyber attacks are difficult to calculate. For example, assigning specific value to intellectual property that is lost during attacks is difficult. Also, how does one even put a price on the value of national secrets, operational plans, or military capabilities when government and military networks are breached? The Lockheed Martin data breach that compromised secret information on the F-35 Joint Strike Fighter exemplifies a single attack that resulted in a loss of intellectual property and exposed military capability.[20]

A third-party network is a network belonging to an entity that is not directly related to or a sub-component of the central entity or organization in question and is not

[17] Adapted from Ibid.

[18] Lori Widmer, "10 Costliest Data Breaches," *National Underwriter/Life & Health Financial Services* 119, no. 7 (July 2015): 46.

[19] Elinor Mills, "Pentagon Spends over $100 Million on Cyberattack Cleanup," *CNET News*, April 7, 2009, http://news.cnet.com/8301-1009_3-10214416-83.html.

[20] Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009, http://www.wsj.com/articles/SB124027491029837401.

involved in the processing, transmission, or storage of data within the central network.[21] Third-party networks can represent a wide range of organizations or entities, but common examples are partner organizations, material supply vendors, service providers, and sub-contractors.[22] Third-party organization networks represent a potential attack vector into the networks of larger organizations they connect to. In many cases, attackers just need to find a soft breach point into a defended network in order to pivot within that network to reach critical or sensitive areas and accomplish their goals. The third-party networks often represent that soft breach point into larger networks. Numerous examples of network breaches through third parties exist and those are discussed further in Chapter II.

Several factors contribute to poor security in third-party networks, but primarily the focus is on cost.[23] Organizations make network security decisions based on cost benefit analyses of the costs to improve network security versus the costs of cyber attacks and network breaches.[24] As will be discussed later, strengthening network security can be an expensive investment. Many private sector companies view this investment as purely a cost and not an investment that can add value to the company and ultimately contribute to cost savings.[25] In short, companies only consider the direct costs of network security investments in their analyses but not any of the intangible benefits these investments may provide. Organizations also often fail to completely consider costs of cyber attacks in their analyses. The difficulties in accurately calculating the true costs of cyber attacks will be discussed in more detail later, but it is something that is very hard to do well. Inaccurate cost calculations will obviously lead to poor cost analyses and affect network security decision making. Additionally, the direct costs to victim organizations associated

---

[21] PCI Security Standards Council, "Information Supplement: Third-Party Security Assurance," 2 (August 2014), https://www.pcisecuritystandards.org/documents/ PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf.

[22] Karen Kroll, "Are Your Business Partners Letting in the Hackers?" *Compliance Week*, November 25, 2014, 64.

[23] John Keller, "Defense Industry Concerned about Cyber Security; Not Sure Where to turn for Help," *Military & Aerospace Electronics* 21, no. 6 (June 2015): 8.

[24] Larry Clinton, "The Value Proposition for Cyber Security: Does It Exist and How Can We Create it," Internet Security Alliance, 4 (2006), http://www.isalliance.org/presentation/ 1_ISA_Overview_Presentations/2006_12_00_Larry_Clinton_Commerce_Department_Presentation.pdf.

[25] Tim Scully, "The Cyber Security Threat Stops in the Boardroom," *Journal of Business Continuity & Emergency Planning* 7, no. 2 (Winter 2013/2014): 140.

with cyber attacks are often diluted, so the victims may not feel the full financial brunt of attacks.[26] This occurs because costs, such as replacing credit cards, may not be directly born by the attacks' victims.[27] Also, things like cyber insurance policies and tax write-offs can serve to lessen the financial impact to cyber attack victims.[28] For these reasons, many organizations fail to see good business value in network security investments and consequently, make network security decisions that leave their networks vulnerable.

One method for network owners to improve the security of their own networks is to promote better security in the third-party networks they connect to. So this thesis specifically focuses on the threat posed by third-party networks, and how the DOD may be able to improve its own network security by assisting and providing incentives for select third parties to improve their network security. This thesis is going to accomplish this objective by analyzing current federal government programs that promote security within the private sector and then make recommendations for how these programs can be used to influence third-party network security.

To further illustrate the threat third-party networks represent to the DOD, the next section will present a short scenario of how an attacker might go about conducting an attack on a DOD network through a third party. This scenario itself is hypothetical, but utilizes an actual TRANSCOM network application as its core element in order to create a scenario that is realistic. The previous TRANSCOM example also demonstrates the applicability of the following scenario.

A. THIRD-PARTY NETWORK ATTACK SCENARIO

This scenario incorporates the U.S. Transportation Command's (TRANSCOM) Single Mobility System (SMS) 10.3.0 website,[29] and the transportation and shipping

---

[26] Ibid., 140–141.

[27] Benjamin Dean, "Sorry Consumers, Companies Have Little Incentive to Invest in Better Cybersecurity," *Quartz*, March 05, 2015, http://qz.com/356274/cybersecurity-breaches-hurt-consumers-companies-not-so-much/.

[28] Ibid.

[29] "SMS," Single Mobility System 10.3.0, accessed April 16, 2016, https://sms.transcom.mil/sms-perl/smswebstart.pl. SMS is a web-based unclassified computer system that provides visibility of air, sea, and land transportation assets.

companies that service TRANSCOM requirements. The SMS site is part of the larger DOD information network (DODIN) and has network links to other parts of the DODIN. The transportation and shipping companies pass information on transportation assets and movement schedules through their individual networks using remote access to SMS. Obviously, information on the movement schedules of U.S. military forces and assets would be an inviting target for many potential attackers, but the link between these companies and the SMS site is also an attack vector into the DODIN. So in this scenario, the transportation companies' networks are the third-party networks and cyber attacks against them represent a more significant risk to the DOD than just the loss of the transportation information. Attacks against these third-party networks represent an increased risk of a breach into the DODIN.

The attackers know they must carefully prepare to succeed in this attack. They start by conducting research, probably Internet-based, on transportation companies that TRANSCOM is currently using.[30] The attackers then conduct reconnaissance, or footprinting,[31] on the companies' networks. In this step, the attackers begin to map the companies' networks, determine what type of IT systems the companies are using, look for email addresses and other company contact information, and look for background information on the companies and their employees. During this initial footprinting, the attackers' goal is to obtain as much background information as possible on these companies. The attackers' next steps are active scans of the companies' networks to scan for open ports, services, and network vulnerabilities using pre-built cyber attack tool kits.[32] They also use these tool kits to execute exploits against any vulnerability they find in an initial attempt to gain access to any of these networks they can. Using information gathered during footprinting, the attackers also likely send malware-laced emails specifically crafted to target select employees in spear fishing attacks against these companies. The successful exploits against network vulnerabilities and malware delivered through the successful spear fishing attacks allow the attackers to gain access to

[30] See Appendix A for results of the author's Google search of TRANSCOM contracts.

[31] Stuart McClure, Joel Scambray, and George Kurtz, *Hacking Exposed*, 7th ed. (New York, NY: McGraw-Hill, 2012), 8.

[32] Ibid., 47.

numerous networks of TRANSCOM's contractors. Once insides these companies' networks, the attackers expand their presence within the networks. The attackers eventually select the transportation company network that provides them the optimal attack vector into the TRANSCOM network.

TRANCOM uses an electronic data interchange (EDI) to transfer information between the transportation company and TRANSCOM's SMS site. Once the attackers have gained access to the transportation company's network, they are able to access the server communicating with the EDI and work through that server using credentials stolen from the transportation company to infiltrate TRANSCOM's SMS site. The attackers now not only have access to valuable DOD transportation information, but more importantly to them, are also able to access the outer edge of the DODIN. The attackers spend time mapping and enumerating the section of the DODIN they have accessed and are eventually able to identify vulnerabilities in the DODIN's internal security structure that should isolate the SMS site from other parts of the DODIN. They may also discover vulnerabilities that allow them escalate the user privileges with which they accessed the DODIN. The attackers then exploit these vulnerabilities and pivot to other parts of the DODIN where they can gather additional information, negatively impact or corrupt data, create backdoors or other access points into the DODIN, or carry out any other objectives they have.

While this exact scenario with the TRANSCOM SMS site and transportation company networks may never come to pass, this type of cyber attack is very plausible. The DOD deals with hundreds of vendors and service providers, with many of these being small companies and businesses that may not have invested in robust network security themselves. As information networks become increasingly interconnected and automated, information exchange is going to occur between the DOD and these third parties via an electronic information exchange. These third parties, particularly those with less secure networks, may provide access to attackers targeting the DODIN and thus, are a risk to DOD network security. While this risk can never be completely eliminated, it can be mitigated by improving the security of third-party networks that interact with the

DODIN. This thesis will identify actions the DOD can take to improve third-party network security and provide recommendations on how to implement them.

B. PURPOSE

The purpose of this thesis is to improve the security of the DODIN by proposing a system that can influence improved network security in third-party networks that exchange information with the DODIN. The research for this thesis will primarily focus on the networks of vendors and contractors who provide products or services to the DOD, however, the recommendations may be applied to any third-party networks that interact with the DODIN. These third-party networks represent a potential security risk to the DODIN. If not secured properly, these third-party networks are potential attack vectors against the DODIN. The ultimate goal of this research is to provide recommendations on actions the DOD can take to influence third-party network owners to improve the security posture of their networks, thus reducing the risk they pose to the DODIN.

C. ANALYSIS METHODS

This thesis uses the systems engineering process and a defense acquisition methodology to analyze and identify specific DODIN security shortfalls and identify system requirements to meet those security shortfalls. Feasible solutions that are affordable are analyzed to recommend a system to the DOD that can fill the operational need created by these shortfalls. Since a detailed analysis of the systems engineering process is given in Chapter II, that material will not be covered in this section. This section merely describes the analysis method used to address this particular problem.

The systems engineering process begins with the definition of problem or a need.[33] Analyzing the previous examples of the risks posed by third-party networks and other similar examples in Chapter II, the problem is the DOD's lack of ability to influence the network security of third-party networks that connect to the DODIN. In the next step, an initial set of top level system requirements are generated from the identified

[33] Benjamin S. Blanchard, *System Engineering Management*, 4th ed. (Hoboken, NJ: John Wiley & Sons, 2008), 51–52.

problem or shortfall.[34] The top-level system requirements to address the problem identified in this thesis are: set specific network security standards for the third-party networks; provide influence mechanisms that can convince third-party networks to meet these network security standards; provide verification mechanisms to ensure third-party networks meet these network security standards; provide reporting mechanisms from third-party networks to the DOD; and function within the larger DODIN network security system-of-systems (SOS).

Once the systems engineering process has identified the need and the system requirements, the DOD uses an acquisition methodology to make a material development decision (MDD), which is whether the DOD will pursue as material or non-material solution.[35] A non-material solution generally manifests in the form of a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) analysis and Joint DOTMLPF-P change request (DCR) validation.[36] A material solution manifests in the form an actual physical system that is acquired through the Defense Acquisition System (DAS).[37] The DOD can obtain a material solution via several methods: procurement or modification of a commercial-off-the-shelf (COTS) or government-off-the-self (GOTS) system; modification of an existing DOD system; or development of a completely new system.[38] The literature reviewed in Chapter II and the analysis in Chapter III shows that the DOD and federal government as a whole have already attempted to address the need for more influence in third-party network security with DOTMLPF-P solutions. Those DOTMLPF-P solutions do not meet the system requirements set previously. No viable material solutions were identified during research, thus this thesis presents a non-material solution to meet these system requirements.

---

[34] Ibid., 19.

[35] Chairman of the Joint Chiefs of Staff (CJCS), *Joint Capabilities Integration and Development System (JCIDS)*, CJCS Instruction 3170.01I, Washington, DC: Chairman of the Joint Chiefs of Staff (CJCS), January 23, 2015, A14-A15.

[36] Ibid., A14.

[37] Ibid.

[38] Under Secretary of Defense (AT&L), *The Defense Acquisition System*, DOD Directive 5000.01, Washington, DC: Under Secretary of Defense (AT&L), 2007, 8.

Consequently, this thesis analyzes recommendations for a DOTMLPF-P solution through modifications in organization, personnel, and policy of an existing DOD system.

The functional analysis in Chapter IV of the proposed system is the final step of the systems engineering process explored in this thesis. This step analyzes the previously set top level system requirements and links them to the proposed system's functions in order to satisfy the DOD's operational need. Thus, the functional analysis of the system set the overall system design and led to recommendations on that design to the DOD.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. INTRODUCTION

Third-party information technology (IT) networks can potentially represent a significant security risk to any large data network. In fact, history has shown large, well-protected networks are often attacked through third parties. Data breaches at Target,[39] Home Depot,[40] and other corporations[41] are prime examples of successful network attacks through third-party networks. This review has six total sections with the first five sections relating to different areas of cyber security that are important for addressing this problem: 1) network vulnerability assessments, 2) cyber security reports, 3) third-party network breaches, 4) U.S. government cyber security actions, and 5) monetary costs of cyber-attacks. The sixth section reviews the systems engineering process. This review provides evidence that third-party networks represent a significant and costly risk to Department of Defense (DOD) data networks, and there are potentially actions the DOD can take to influence the security of those third-party networks. The information from this review supports the arguments that aim to propose strategies the DOD can utilize to influence third-party network owners to improve the security of their networks.

B. NETWORK VULNERABILITY ASSESSMENTS

This section of the literature review specifically focuses on one aspect of computer network security; network vulnerability assessments. Network vulnerability assessment as a topic is well-studied, and there has been a significant amount written on it. The goal of this review is to identify specific non-proprietary vulnerability assessment tools the DOD could share with third-party network owners for use on their own networks. In general, a vulnerability assessment is simply an analysis of a system to

[39] Senate Committee on Commerce, Science, and Transportation, "A Kill Chain Analysis of the 2013 Target Data Breach," i.

[40] Kerner, "Home Depot Breach Expands, Privilege Escalation Flaw to Blame."

[41] Kroll, "Are Your Business Partners Letting in the Hackers?" 64.

identify, quantify, and prioritize system vulnerabilities.[42] For the purposes of this review, that system is an information network. The National Institute of Standards and Technology (NIST) recognizes the importance of continually testing networks for vulnerabilities so they can be corrected before they can be exploited.[43] Pandey et al., recognize the four phases of network assessment as reconnaissance, network scanning, vulnerability assessment, and exploitation.[44] Vulnerability assessment tools are utilized to uncover specific network weaknesses so that corrective action may be taken before an attacker is able to exploit the weaknesses. Vulnerability assessment tools come in two main flavors, network scanners and vulnerability scanners.[45]

Network scanners, also called network discovery or host discovery tools,[46] are designed to either actively or passively scan networks and hosts to discover open and active ports and services according to Pandey et al.[47] Attackers can potentially use open ports as avenues to penetrate networks. Network scanners can identify ports that network administrators may not know are open. If these ports are not required to be open for normal network operations, network administrators can close them, thereby eliminating potential attack vectors. Common network scanners include NMAP, Superscan, Cain,[48] Portqry, Nbtscan,[49] and others.

Vulnerability scanners are designed to assess a network for known vulnerabilities in the network structure, and in network hosts, which have not yet had patches applied.[50]

---

[42] Sudhir K. Pandey et al., "Implementation of A New Framework for Automated Network Security Checking and Alert System," *2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN)*, (2014): 4, doi: 10.1109/WOCN.2014.6923089.

[43] Aniwat Hemanidhi et al., "Network Risk Evaluation from Security Metric of Vulnerability Detection Tools," *2014 IEEE Region 10 Conference*, (2014): 2, doi: 10.1109/TENCON.2014.7022358.

[44] Pandey et al., "Implementation of A New Framework for Automated Network Security Checking and Alert System," 1.

[45] Ibid., 1–2.

[46] Stuart McClure, Joel Scabray, and George Kurtz, *Hacking Exposed*, 53, 55.

[47] Pandey et al., "Implementation of A New Framework for Automated Network Security Checking and Alert System," 3.

[48] Stuart McClure, Joel Scabray, and George Kurtz, *Hacking Exposed*, 49, 51, 55.

[49] Pandey et al., "Implementation of A New Framework for Automated Network Security Checking and Alert System," 5.

[50] Ibid., 2.

Vulnerability scanners work based on known system, either software or hardware based, vulnerabilities that are stored in their databases. Pandey et al. says a given system type can have many hundreds or more known vulnerabilities.[51] Scanning large networks with potentially thousands of systems that can each have potentially hundreds or thousands of vulnerabilities is obviously a large task. Hemanidhi et al. claim that as speed in discovering and patching vulnerabilities in networks is critical, automated high speed scanning tools are desired.[52] Yoon and Sim (2007) note that vulnerability scanning tools can also be active or passive, and both varieties are sometimes used as they each have negatives and positives.[53] Often, these assessment tools have the means to rank vulnerabilities based on their severity level to allow network administrators to prioritize the corrective actions they need to take. Common vulnerability scanners include Nessus, Retina,[54] OpenVas, NMAP,[55] and others.

Research from Yoon and Sim (2007), Hemanidhi et al. (2014), and Pandey et al., (2014) has definitively shown that multiple tools working in concert produce a much more thorough assessment.[56] Individual network scanners and vulnerability scanners have their own strengths and weaknesses; using only one will likely leave gaps in the overall vulnerability assessment. These gaps might be found and exploited by an attacker using different tools.

Network vulnerability assessments are key component of both attack and defense strategies in information networks. Actual network vulnerability scanners are a tool DOD can offer to third-party network owners to aid them in incorporating network vulnerability assessments into their network defense strategies. Thus, providing access to

---

[51] Ibid., 2.

[52] Hemanidhi et al., "Network Risk Evaluation from Security Metric of Vulnerability Detection Tools," 1.

[53] Jun Yoon and Wontae Sim, "Implementation of the Automated Network Vulnerability Assessment Framework," *4th International Conference on Information Technology, 2007*, (2007): 154, doi: 10.1109/ IIT.2007.4430423.

[54] Hemanidhi et al., "Network Risk Evaluation from Security Metric of Vulnerability Detection Tools," 1.

[55] Stuart McClure, Joel Scabray, and George Kurtz, *Hacking Exposed*, 87–88.

[56] Ibid., 153. See also Hemanidhi et al. (2014) and Pandey et al. (2014).

these assessment tools to third-party network owners becomes part of the thesis's incentivized influence strategy.

C. CYBER SECURITY REPORTS

Reviewing cyber security reports is important to this review as these reports can be used to help grasp the enormity of the risks that cyber-attacks represent to both the DOD and the private sector and providing justification for both to cooperate in mutual defense initiatives. This review specifically searched for information on cyber-attacks using third-party networks as attack vectors or cyber-attacks conducted by third-party network owners themselves. Both of these are related in that the attackers use the third-party network as conduit for the attack.

In 2012, the Defense Science Board (DSB) produced a report reviewing and providing recommendations on the resiliency of DOD systems to cyber-attack. In the report, the DSB describes the cyber threat by dividing it into three classes of varying sophistication. The DSB uses the cyber attackers' level of resourcing and sophistication in using either known tools and vulnerabilities or creating their own to make class determinations.[57] These threat classes are then used to create a basic taxonomy of the attackers by dividing them into six distinct tiers,[58] which serves as an attempt to identify and define the overall cyber threat. Table 2 defines each threat tier and Figure 1 depicts the DSB's overall attacker taxonomy:

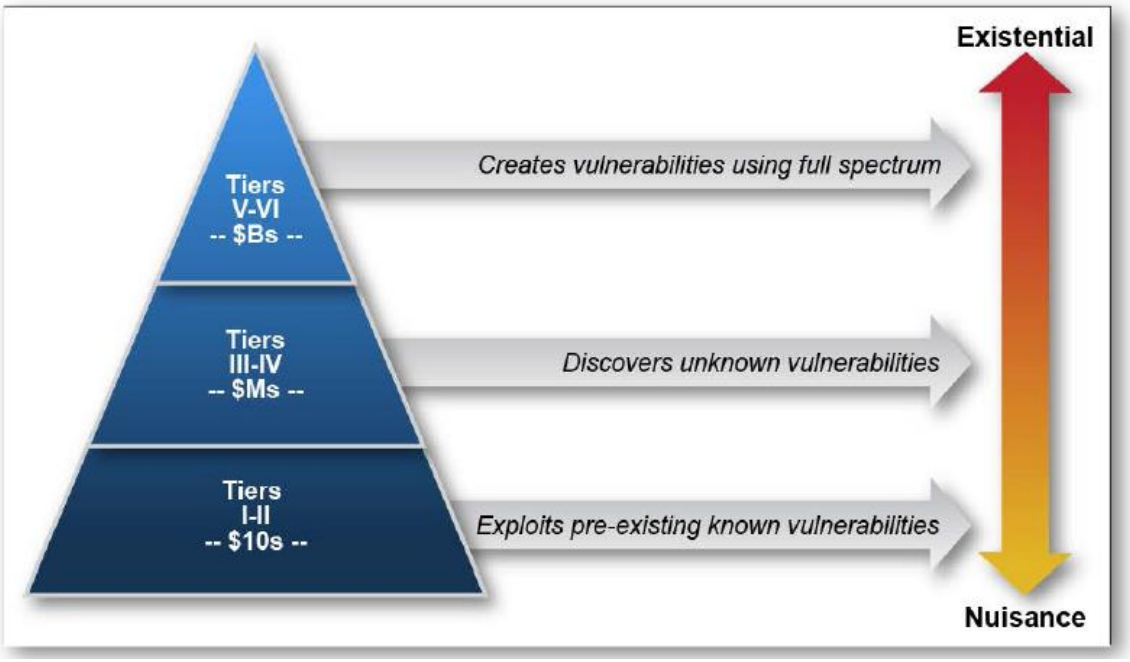
[57] Defense Science Board Task Force on Resilient Military Systems, *Resilient Military Systems and the Advanced Cyber Threat*, 21, (2013), http://www.acq.osd.mil/dsb/reports/ ResilientMilitarySystems.CyberThreat.pdf.

[58] Ibid., 22.

Table 2. Description of Cyber Threat Tiers[59]

I	Practitioners who rely on others to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits).
II	Practitioners with a greater depth of experience, with the ability to develop their own tools (from publically known vulnerabilities).
III	Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode root kits10, frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.
IV	Criminal or state actors who are organized, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits.
V	State actors who create vulnerabilities through an active program to "influence" commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.
VI	States with the ability to successfully execute full spectrum (cyber capabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic, etc., domains and apply at scale.

[59] Source: Ibid., 22–23.



Dollar figures represent the nominal investment amount required to operate at a given tier.

Figure 1. Cyber Threat Taxonomy[60]

The report then moves on to describe the possible consequences to both U.S. military forces and the United States at large in the face of sophisticated sustained attacks. These include the degradation of operational performance and erosion of trust in information systems for the U.S. military, and the breakdown of basic civil services inside the nation.[61] The DSB attempts to set the expectation that networks and systems can never be made completely secure and that a threshold of "good enough"[62] based on threat parameters and mission requirements should be set for cyber security. The report then moves into its recommendation section in which there are many that cover a wide range of capabilities. The DSB also provides monetary and timeframe estimates to implement the DSB's recommendations. Table 3 depicts the DSB's estimates to implement its recommendations:

[60] Source: Ibid., 21.

[61] Ibid., 28.

[62] Ibid., 30.

Table 3. Defense Science Board's Estimated Cyber Security Investment Requirements[63]

		Cost	Timeframe
1	Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack).	>$500M/yr	36-60 mo.
2	Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary.	>$500M/yr	36-60 mo.
3	Refocus Intelligence Collection and Analysis to Understand Adversarial Cyber Capabilities, Plans and Intentions, and to Enable Counterstrategies.	<$50M/yr	12-24 mo.
4	Build and Maintain World-Class Cyber Offensive Capabilities (with appropriate authorities).	$50M-$100M/yr	12-24 mo.
5	Enhance Defenses to Protect Against Low and Mid-Tier Threats.	<$50M/yr	6-18 mo.
6	Change DOD's Culture Regarding Cyber and Cyber Security.	<$50M/yr	12-48 mo.
7	Build a Cyber Resilient Force.	$50M-$100M/yr	12-24 mo.

The Verizon Enterprise produces an annual data breach investigation report. The 2014 report, which covered network data breaches and security incidents recorded in 2013, was used for this research.[64] The report focused on corporate world, but it is still useful for this study as threats and trends identified here are relatable to the DOD as well. The report broke the sample data down into a wide array of statistics covering categories such as attack methods, target types, time to complete attacks, time to discover attacks and breaches, breach discovery methods, motive for attacks, and others. The report also compares like statistical categories from the 2013 data against previous years' data. From these statistics, the report was able to identify several overarching patterns. In fact, the team was able to group 94 percent of all network breaches in 2013 into one of nine categories.[65] After analyzing previous years' data, the team found a similar percentage of

[63] Adapted from Ibid., 82.

[64] Verizon Enterprise, "2014 Data Breach Investigations Report," 13.

[65] Ibid., 13.

attacks from these years could also be grouped to the same nine categories. Table 4 displays these categories and their relative occurrence percentages:

Table 4. Verizon Data Breach Investigations Report's Network Breach Category Patterns[66]

Category	2013 Breaches	2011-2013 Breaches
Point-of-Sale (POS) Intrusions	14%	31%
Web App Attacks	35%	21%
Insider Misuse	8%	8%
Physical Theft/Loss	<1%	1%
Miscellaneous Errors	2%	1%
Crimeware	4%	4%
Card Skimmers	9%	14%
Denial-of-Service (DOS) Attacks	0%	0%
Cyber-espionage	22%	15%
Everything else	6%	5%

For 2013, n = 1,367 breaches.

For 2011–2013, n = 2,861 breaches.

More importantly for this study, the report presented findings related to third parties or third-party networks. The report identified that in a significant percentage of corporate cases an attack would originate in an individual store, and the attacker would then use that access to penetrate the corporate networks.[67] As the store network and corporate network are often separate, this can be viewed as an attack through a third-party network. As indicated in the report, remote access software to support third-party access to corporate networks also seems to be a commonly shared threat vector in many attacks.[68] Consequently, Verizon Enterprise recommends corporations limit third-party access to their networks, ensure all vendors and service providers are clear when they

[66] Adapted from Ibid., 14.

[67] Ibid., 17.

[68] Ibid., 19.

should access the corporate network to complete their third-party duties, and corporations should institute multi-factor authentication procedures for their networks.[69]

The Defense Security Service (DSS) published its 2015 annual report on the targeting of cleared U.S. defense contractors by those attempting to gain information on U.S. military technology. The report's dataset consisted of self-reporting by the cleared contractors for 2014 incidents. DSS notes that reporting from the defense industry has been steadily increasing, 8 percent alone from 2013 to 2014 datasets.[70] Similar to other reports, the DSS broke their data set into different statistical categories. The data was also divided into subsets based on six geographical regions and comparisons were made among the different regions. The report listed electronics as the most targeted technology category.[71] As reporting from cleared contractors has increased, DSS is getting a clearer picture of the threats against the U.S. defense industrial base. DSS believes foreign entities are still motivated to gain information on U.S. critical technologies, and DSS assesses attacks against cleared contractors to gain that information will continue for the foreseeable future.[72] DSS predicts cyber-attacks will continue to be one of the preferred means to target cleared contractors, and the attackers will almost certainly use employees,[73] sub-contractors, service providers, and vendors (third parties) as attack vectors.

Reports from several additional sources such as McAfee Labs that produces a quarterly threat report and the U.S. Army War College, Strategic Studies Institute (SSI) that completed a study on Cyber infrastructure protection were reviewed for this research. These reports provided different statistics, trends, and conclusions on cyber-attacks and threats. One McAfee report listed numerous recommended policies and procedures for

---

[69] Ibid., 19.

[70] Defense Security Service, *2015 Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting*, 10, (2015), http://www.dss.mil/ci/ci_reports.html.

[71] Ibid., 19.

[72] Ibid., 44.

[73] Ibid., 45.

data protection.[74] The Army War College report contained a useful data point on attacks by third parties on networks. The report stated three industry-leading data aggregation companies were each attacked and their networks breached in the 2003 to 2005 timeframe.[75] In each case, other entities in business with these companies were able to access their networks and steal data, with one of the companies being breached twice and losing over a billion records total.[76]

Cyber security reports are important because they give a perspective of the overall cyber threat environment that exists today. Also, almost all these cyber security reports had some reference relating to third-party networks, which served to highlight the risks they pose to other organizational networks. Thus, these cyber security reports strengthen the claim that third-party networks pose a security risk to DOD networks.

D. THIRD-PARTY NETWORK ATTACKS

Several pieces of literature specifically addressed network attacks executed through third-party networks. This should not be surprising, considering several high profile corporate network breaches have used third-party networks as attack vectors. Most notably was the Target corporation breach, but others such as Home Depot, several large hotel chains, Barclay's,[77] AT&T, Goodwill, and others[78] have been successfully attacked through third parties as well.

According to the Senate Committee on Commerce, Science, and Transportation report, the Target network was first breached by the attackers on November 12, 2013, and the attackers where not removed from the Target network until December 15, 2013.[79]

---

[74] McAfee Labs. *McAfee Labs Threat Report*, 25, (August, 2015), http://www.mcafee.com/us/mcafee-labs.aspx.

[75] Tarek Saadawi and Louis Jordan, eds., "Cyber Infrastructure Protection," 52, (2011), www.strategicstudiesinstitute.army.mil/pdffiles/PUB1067.pdf.

[76] Ibid., 52–53 & 57.

[77] Penny Crosman, "Target Breach Was Months in the Making," *American Banker*, February 12, 2014, 1, http://search.proquest.com/docview/1497400210?accountid=12702.

[78] Kroll, "Are Your Business Partners Letting in the Hackers?" 64.

[79] Senate Committee on Commerce, Science, and Transportation, "A Kill Chain Analysis of the 2013 Target Data Breach," 12.

The attackers penetrated Target's network by first stealing access credentials from an HVAC service provider who had remote access to Target's electronic billing system.[80] The attackers sent malware-infected email to the HVAC service provider to steal the access credentials and were then able to exploit a default billing account with those credentials.[81] The Senate Committee report indicated a leading theory as to how the attackers discovered the HVAC service provider was simple Internet searches for Target's vendors and service providers.[82] Similarly, reporting by Kerner shows the Home Depot network was also breached when a third-party vendor who had remote access to the company's network had their access credentials compromised.[83] An article by Crosman has the same scenario for the hotel chain breaches where a common sub-contractor's network was breached, allowing the attackers to steal access credentials to each of the hotel chains' networks.[84]

Estimates vary, but a conservative one according to Kroll is that one third of all network attacks are somehow linked to current or former vendors, sub-contractors, service providers, or other third parties, and only 44 percent of network administrators have a formalized process for evaluating the risk posed by third-party networks that contact their own networks.[85] Even very tangential relationships can pose a risk. A large oil firm was attacked using a popular Chinese restaurant network as an attack vector because the oil firm's employees routinely accessed the restaurant's website for its online menu.[86]

Most large organizations allow some type of third-party access to their networks as these third parties provide some type of required service for the organization. Goldstein says this access to networks can provide an easier attack vector for the

---

[80] Ibid., 4.

[81] Ibid., 8, 10.

[82] Ibid., 7.

[83] Kerner, "Home Depot Breach Expands, Privilege Escalation Flaw to Blame."

[84] Crosman, "Target Breach was Months in the Making," 64.

[85] Kroll, "Are Your Business Partners Letting in the Hackers," 64.

[86] Ibid., 64.

attacking entity.[87] An attack vector through a third-party network is attractive because large corporations and government networks are typically better protected and represent a relatively hard target. However, networks belonging to smaller entities providing services to these corporations or the government are often much less protected, and represent a potentially less defended access point to the larger network.[88] Goldstein highlights that a cautious network administrator will only view their network security as being as good as the security of the third-party networks their networks interact with.[89]

To mitigate the threats from third-party networks, network administrators can take several actions. First, as noted in the previous section on cyber security reports, cyber security experts recommend network administrators should have multi-factor authentication procedures in place for all third parties with remote access to their networks.[90] Goldstein also recommends administrators for large networks require third parties conduct self-assessments of their networks, but he notes this option has significant drawbacks, not the least of which is ensuring the third party actually accomplishes the assessments or has the technical capability to effectively conduct a self-assessment.[91] Goldstein notes a more thorough option would be for the larger entity to have their own network administrators carry out the assessment function on the third party or hire a cyber security firm to conduct the assessment.[92] Since this option could potentially be very time consuming and resource intensive depending on the number of third parties that connect to a larger network, there is another more refined option. Third parties should be assessed by their level of remote access to a larger network, as well as, the type of data they hold or have access to. The third parties are then ranked by the level of risk they

---

[87] Daniel J. Goldstein, "Amid Cyber Threat to your Business Data, Trust but Verify Third-Party Processing," *Mortgage Banking*, July 2015, 85.

[88] Kroll, "Are Your Business Partners Letting in the Hackers," 64.

[89] Goldstein, "Amid Cyber Threat to your Business Data, Trust but Verify Third-Party Processing," 85.

[90] "Working with third-parties: Make Security a Priority," *SC Magazine: For IT Security Professionals* (UK Edition), July-August 2014, 8. http://www.scmagazineuk.com/working-with-third-parties-make-security-a-priority/article/357460/.

[91] Goldstein, "Amid Cyber Threat to your Business Data, Trust but Verify Third-Party Processing," 86.

[92] Ibid., 86.

present to the larger network. The larger entity then conducts targeted assessments of a certain number of the highest risk third parties on an annual basis.[93]

The literature reviewed in this section specifically highlights the risks third-party networks can represent. This risk to other organizational networks is the foundational problem addressed in this thesis. Third-party network vulnerabilities present a direct risk to the DOD just as they do to any other organization that allows third-party connections to their networks. So this section serves as the foundation for this research.

E. U.S. GOVERNMENT CYBER SECURITY ACTIONS

Since network data breaches have been such a headline grabbing issue in recent years, it is not surprising there have been numerous government actions, initiatives, and policy changes in an attempt to improve security within both government and civilian networks. This work also follows that theme and focuses on how the DOD can induce improvement in third-party networks. Specifically, this portion of the study focuses on government actions that primarily affect civilian networks.

The legislative front seems to be an area where there has not been a great deal of governmental action. The Data Security Act was a bi-partisan bill introduced in the Senate in 2014, and was written to set national standards for securing personal information collected by organizations,[94] but it ultimately never passed the Senate. The bill was introduced in the 2015 Senate session, but as of this writing was still stuck in committee so its prospects for passage are low.[95] The National Defense Authorization Act (NDAA) of 2013, contained language dealing with data and network security of cleared defense contractors. The NDAA required the Secretary of Defense to emplace procedures to require cleared defense contractors to "rapidly" report to the DOD when

---

[93] Ibid.

[94] Victoria Finkle, "Lawmakers Unveil Data Security Bill, Citing Target Breach," *American Banker*, January 16, 2014, 1, http://search.proquest.com/docview/1490680935?accountid=12702.

[95] "S. 961: Data Security Act of 2015," GovTrack.us, Accessed December 2, 2015, https://www.govtrack.us/congress/bills/114/s961.

their networks were penetrated.[96] The NDAA also required procedures be enacted that would allow DOD personnel to request and obtain network information from cleared defense contractors for post attack forensic analysis.[97] Nothing in the NDAA actually sets standards or mandates improved contractor network security, which is the issue this thesis will address.

There are initiatives on the scientific front that have the potential to improve software security standards. Underwriters Laboratories (UL) is considering expanding its scope beyond safety testing and move into software security testing.[98] While software is not a network, and UL is not a governmental agency, there is a regulatory connection, and this could improve and enforce general cyber security standards, thus it is mentioned here. Additionally, the White House's Office of Science and Technology Policy is studying the possibility of establishing an independent laboratory for testing new and existing software against established cyber security standards.[99] Again this initiative could improve the enforcement of cyber security standards.

The majority of cyber security actions have come from various entities within the executive branch. Executive Order 13636 of February 12, 2013 ordered government agencies to begin several initiatives. First, the Department of Homeland Security (DHS) and DOD were directed to establish procedures to begin sharing cyber security information with critical infrastructure owners and operators, and it allowed the federal government to bring private sector cyber security experts into the federal government temporarily.[100] The order directed the Director of the National Institute of Standards and Technology (NIST) to establish a framework to mitigate cyber threats to critical

---

[96] United States Congress, *National Defense Authorization Act for Fiscal Year 2013*, 112th Congress, 259–260, (2012) http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf.

[97] Ibid., 259.

[98] "UL, Cited as Model for Cyber Testing, has own Initiative Underway," *Inside Cybersecurity*, July7, 2015, 1, http://search.proquest.com/docview/1694696588?accountid=12702.

[99] "White House Science Office Spurs Effort to Create Cyber Certification Lab," *Inside Cybersecurity*, June 30, 2015, 1, http://search.proquest.com/docview/1692270352?accountid=12702.

[100] Presidential Executive Order 13636-Improving Critical Infrastructure Cybersecurity, *Federal Register*, 11739-11740 (February 13, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

infrastructure.[101] Lastly, it directed the DOD and General Services Administration (GSA) to investigate the feasibility of incorporating cyber security standards into acquisition planning and contract administration.[102]

As a direct result of EO 13636, DHS created the Critical Infrastructure Cyber Community C³ Voluntary Program (originally called Enhanced Cybersecurity Services program).[103] The program allows critical infrastructure owners and operators to receive real time information on cyber security threats and technical assistance in implementing the NIST cyber security framework.[104] Also, the DOD created the voluntary Defense Industrial Base (DIB) Cyber Security and Information Assurance (CS/IA) program. The program is designed to protect unclassified DOD information[105] by allowing cleared defense contractors to receive unclassified and classified cyber threat information from the DOD that they can use to strengthen their networks.[106] Lastly, as directed in EO 13636, NIST created the cyber security framework for critical infrastructure.[107]

The Defense Acquisition Regulations Supplement (DFARS) Clause 252.204-7012 is directly aimed at mitigating risk to government information held by government contractors. The clause currently requires defense contractors to adequately protect unclassified controlled technical information (UCTI).[108] The clause defines adequate

---

[101] Ibid., 11740-11741.

[102] Ibid., 11742.

[103] Robert Nichols, et al., "Cyber Security for Government Contractors," *Briefing Papers* 14 no.5 (April 2014): 9–10, https://www.cov.com/files/Publication/42df1e52-f857-4459-8e3b-41383ca6919f/Presentation/PublicationAttachment/313eea21-adca-4e00-8eac-561a6f0d15a6/Cybersecurity_for_Govt_Contractors.pdf.

[104] United States Computer Emergency Readiness Team, *C3 Voluntary Program, C³ Voluntary Program Outreach and Messaging Kit: Cyber Risk Management Primer for CEOs*, (n.d.), https://www.us-cert.gov/ccubedvp.

[105] Assistant Secretary of Defense (NII), *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*, DOD Instruction 5205.13, Washington, DC: Assistant Secretary of Defense (NII), January 29, 2010, 1.

[106] Department of Defense, *DIB Cybersecurity Activities Fact Sheet: DOD – DIB Cybersecurity Information Sharing Program Overview*, (October 6, 2015), http://dodcio.defense.gov/.

[107] Nichols et al., "Cyber Security for Government Contractors," 10.

[108] Department of Defense, Defense Federal Acquisition Regulations Supplement, Clause 252.204-7012. *Safeguarding of Unclassified Controlled Technical Information*. (November 2013). http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm.

protection as contractors implementing network security protocols that meet NIST Special Publication (SP) 800–53 security controls, explaining to the contracting officer how NIST controls do not apply, or how an alternative measure is equivalent to the NIST controls.[109] Lastly, it requires reporting to the DOD within 72 hours of any cyber incident that affects government UCTI held on the contractor's network.[110]

Related to the DFARS, the Office of Management and Budget (OMB) just this year has proposed changes to the Federal Acquisition Regulations (FAR) to provide guidance to federal agencies on cyber security protections in their contract clauses for acquisitions.[111] OMB closed the comment period on the proposed changes in September 2015[112] and is now creating a memorandum to officially incorporate the final changes into the FAR. The changes will implement new security controls for controlled unclassified information (CUI) on contractor networks, cyber incident reporting by the contractors, network security assessments of the contractor networks, and requirements to follow NIST SP800-171.[113] The FAR change also provides specific contracting language guidance to federal agencies in the three areas listed previously.

The ability to properly assess and mitigate risk is another critical aspect of network security. The cyber risk equation is a conceptual tool that can assist network administrators and owners with this task:[114]

$$Risk = \frac{Threat\ x\ Vulnerability\ x\ Impact}{Security\ Controls}$$

This tool is conceptual, since a network administrator cannot input actual numerical values for the independent variables and compute a numerical value for the risk. However, it does assist the network administrator in conceptually understanding the

---

[109] Ibid.

[110] Ibid.

[111] Office of Management and Budget. *Improving Cybersecurity Protections in Federal Acquisitions*. (n.d.). https://policy.cio.gov/.

[112] Ibid.

[113] Ibid.

[114] John D. Fulp, "Network Security Core Principles," (lecture slides, Naval Postgraduate School, Monterey, CA, February 2016) 10.

overall risk to a network and mitigating that risk to a level acceptable to the network's owning organization.[115] A network administrator has the least amount control over the threat and impact variables.[116] Consequently, the network administrator can mitigate the risk to the network by decreasing the number of network vulnerabilities and increasing the network's security controls.[117]

The objective of this research is to identify shortfalls in government systems that address cyber security, generate system requirements for a new system to fill these shortfalls, design a new system that can fill these shortfalls, and make recommendations to the DOD on how to build and implement that new system. Consequently, reviewing government actions and policy initiatives enacted to date assists in identifying shortfalls in the current government system and in generating the new system requirements. Thus, the research in this area set the foundation for the system design and recommendations in following chapters.

F. FINANCIAL ASPECTS OF CYBER ATTACKS

Literature in this category supports the cost analysis of the proposed actions in Chapter IV. This literature can also assist in decisions on appropriately balancing the level of risk the DOD is willing to accept to the DODIN. Estimates on the monetary impacts of cyber-attacks vary widely. Sabovich and Borst provide the LoveLetter virus as an example of a single virus that circulated worldwide, and had estimated global costs that potentially reached over a billion dollars.[118] The Center for Strategic and International Studies (CSIS) places annual global losses likely around $400 billion, but acknowledge even their own estimates vary widely.[119] The CSIS research also indicates that cyber attack costs for individual nations can range from 0.5 percent to 1 percent of

---

[115] Ibid., 11.

[116] Ibid., 12.

[117] Ibid.

[118] Jason R. Sabovich and James A. Borst, "Remediating Third-Party Software Vulnerabilities on U.S. Army Information Systems" (master's thesis, Naval Postgraduate School, 2012) 16.

[119] Center for Strategic and International Studies (CSIS), "The Economic Impact of Cybercrime and Cyber Espionage," 3 (2013).

gross domestic product (GDP) on the high end to possibly as low as 0.14 percent on the low end of the scale.[120] Table 5 from the CSIS study shows a broader view of these estimates and compares them against other elicit activity for scale:

Table 5. Cyber Attack Costs versus Other Illicit Activities[121]

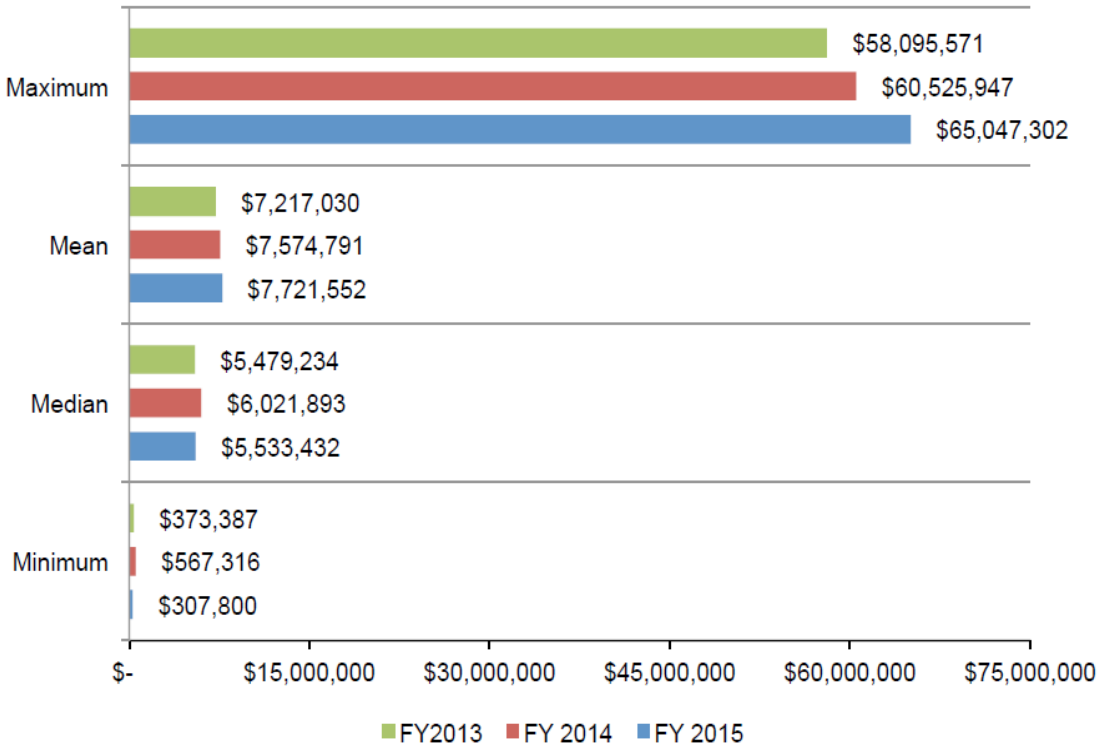
Putting Malicious Cyber Activity in Context			
Criminal Action	Estimated Cost	Percent of GDP	Source
Global			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global Cyber Activity	$300 billion to $1 trillion	0.008% to 0.02%	Various
U.S. Only			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US Cyber Activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Additionally, Lloyd's of London agrees with the $400 billion estimate for global cyber attack costs.[122] Figure 2 depicts estimates by the Ponemon Institute on the annual cost of cyber attacks to the companies participating in its annual cyber crime study and indicates the costs to the surveyed companies have increased over the past several years. So, even though accurate estimates of cyber attack costs are difficult to obtain, research does indicate the costs to companies, national economies, and the global economy are significant.

[120] Ibid., 16.

[121] Source: CSIS, "The Economic Impact of Cybercrime and Cyber Espionage," 5.

[122] Stephen Gandel, "Lloyd's CEO: Cyber attacks Cost Companies $400 Billion Every Year," *Fortune*, January 23, 2015, http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/.



Consolidated view, n = 252 separate companies

Cost expressed in U.S. dollars

Figure 2. The Cost of Cyber Crime[123]

The accurate estimation of cyber attack costs is difficult for several reasons. The CSIS report points out that in many cases organizations may not even realize they have been attacked and suffered losses. In other cases, organizations may try to conceal losses from cyber attacks. Lastly, in many cases, calculating the value of information stolen in cyber attacks is extremely difficult.[124] So to make any estimate, analysts must make cost assumptions. Thus, the estimates vary because different analysts making different cost assumptions produce differing estimates. These estimates include hard costs and soft costs. Sabovich and Borst point out that hard costs are generally easier to calculate and

[123] Source: Ponemon Institute, sponsored by Hewlett Packard, "2015 Cost of Cyber Crime Study: Global," 6 (2015).

[124] CSIS, "The Economic Impact of Cybercrime and Cyber Espionage," 3.

include technician costs, hardware replacement costs, and network upgrade costs.[125] Conversely, soft costs are intangible and thus, more difficult to calculate accurately. Soft costs can include such components as lost opportunity, lost productivity, and lost person hours.[126] However, others may include additional cost components such as government assessed penalties, litigation costs,[127] increased insurance premiums,[128] and reputational damage.[129] Intangible costs to the DOD could be represented by loss of operational security of controlled unclassified or classified information represented by the TRANSCOM[130] and Joint Strike Fighter[131] examples discussed previously. Also, other authors use different terms to describe cyber attack costs. For example, Bernik describes them as direct and indirect costs,[132] and the Ponemon Institute uses the monikers "internal" and "external" to describe costs;[133] as shown in the institute's visual framework of cyber crime costs that is illustrated in Figure 3. This disparity in terminology usage as well as differing assumptions and variables, shows why cyber attack costs estimates vary so widely.

---

[125] Sabovich and Borst, "Remediating Third-Party Software Vulnerabilities on U.S. Army Information Systems," 16

[126] Ibid., 17.

[127] Michael Clark and Charles Harrell, "Unlike Chess Everyone must continue Playing after a Cyber Attack," *Journal of Investment Compliance* 14, no. 2 (2013): 9–10.

[128] G. Steven Smith and Anthony J. Amoruso, "Using real Options to value Losses from Cyber Attacks," *Journal of Digital Asset Management* 2, no. 3/4 (May 2006): 152.

[129] CSIS, "The Economic Impact of Cybercrime and Cyber Espionage," 8.

[130] Senate Committee on Armed Services, Inquiry in Cyber Intrusions Affecting U.S. Transportation Command Contractors, 113th Cong., i.

[131] Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009, http://www.wsj.com/articles/SB124027491029837401.

[132] Igor Bernik, "Cybercrime: The Cost of Investments into Protection," *Journal of Criminal Justice and Security* 16, no. 2 (2014): 109.

[133] Ponemon Institute, sponsored by Hewlett Packard, "2015 Cost of Cyber Crime Study: Global," 3–4 (2015).

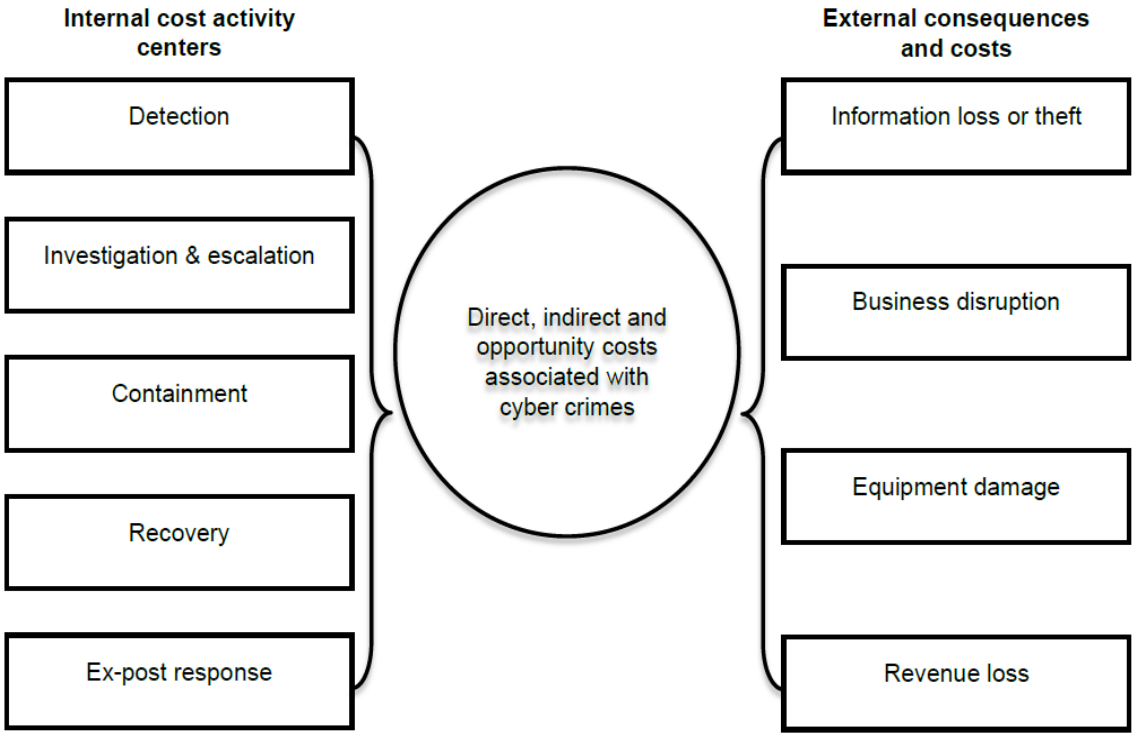
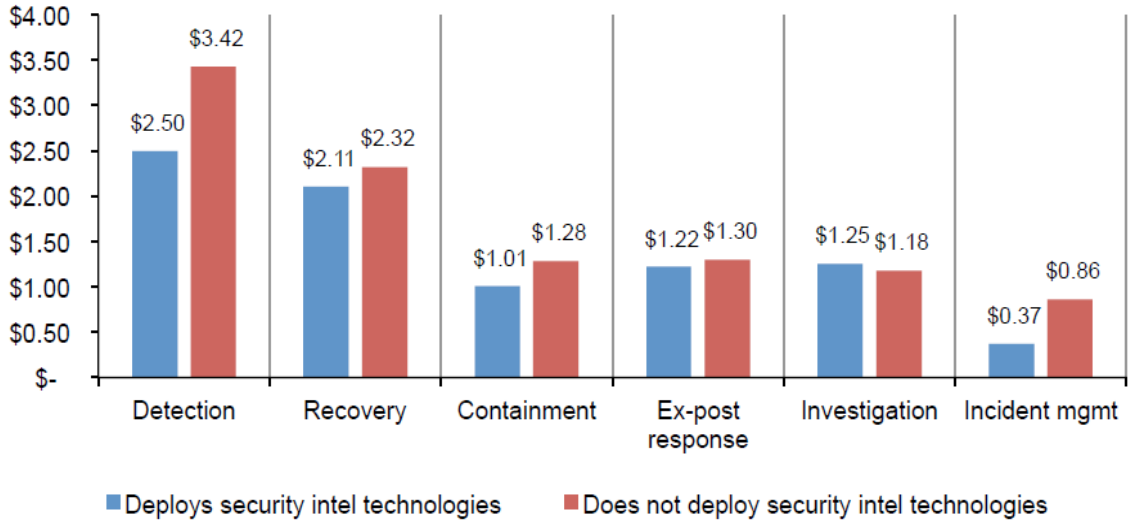


Figure 3. Cost Framework for Cyber Crime[134]

The Ponemon Institute research does seem to indicate that by taking security measures, organizations can reduce the costs they suffer due to cyber attacks. For the companies participating in the study, those that utilized some form of security intelligence system, enterprise security governance practices, and security enabling technologies saw the larges overall reduction in costs associated with cyber attacks.[135] The Ponemon study produced Figure 4, which shows the average amount companies saved by using a network security intelligence system in six different actions to resolve a cyber attack:

[134] Source: Ponemon Institute, "2015 Cost of Cyber Crime Study: Global," 22.

[135] Ibid., 4–5.

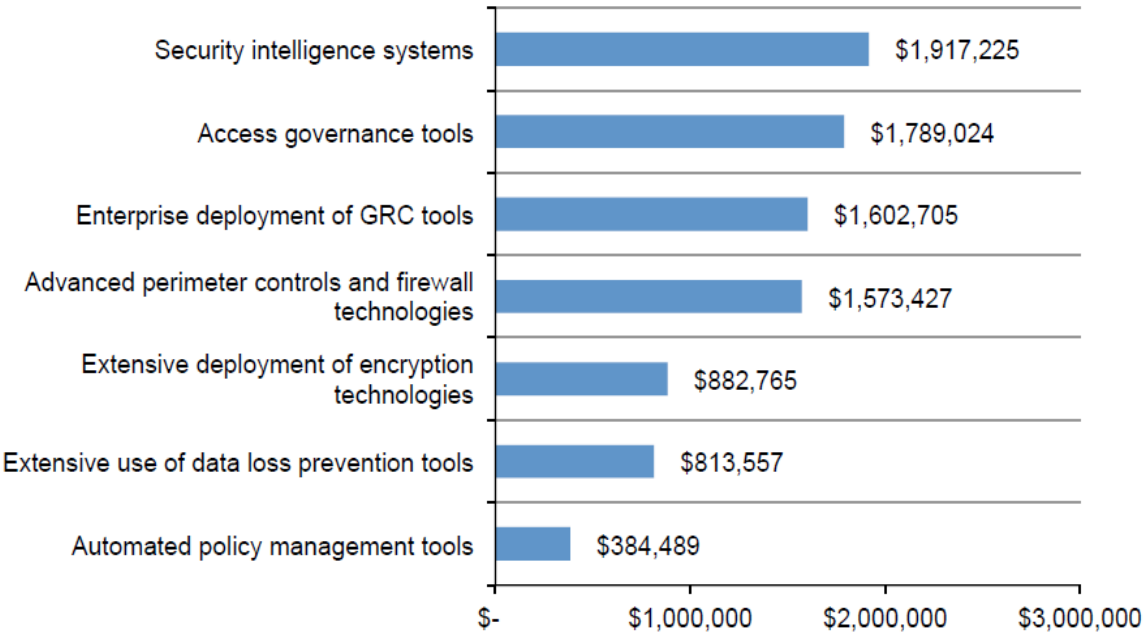


Cost expressed in millions of U.S. dollars, n = 252 separate companies

Figure 4. Activity Cost Comparison and the Use of Security Intelligence Technologies[136]

The Ponemon study also produced Figure 5, which shows potential cost savings companies can realize by utilizing certain network security technologies. The savings represented in Figure 5 are not necessarily cumulative, but individually, represent what components of network security companies should consider investing in:

[136] Source: Ponemon Institute, "2015 Cost of Cyber Crime Study: Global," 18.

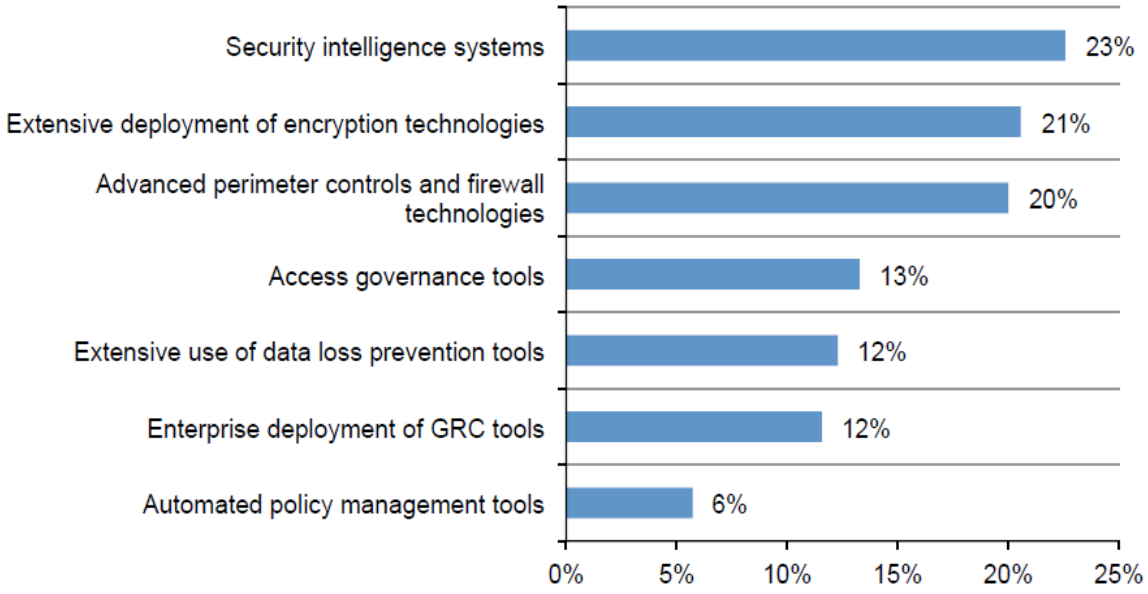


Savings are expressed in U.S. dollars. Consolidated view, n = 252 separate companies.

Figure 5. Cost Savings When Deploying Seven Enabling Technologies[137]

Unfortunately, some of these gross cost savings will be negated by the cost of deploying these security measures. Organizations must use a cost/benefit approach to determine the appropriate type and level of security measures to employ. However, Figure 6 illustrates the return-on-investment (ROI) the Ponemon Institute calculated, using both the cost savings and cost of the technology investment, these companies would achieve if they implemented the following security technologies:

[137] Source: Ponemon Institute, "2015 Cost of Cyber Crime Study: Global," 19.



Consolidated view, n = 252 separate companies

Figure 6. Estimated ROI for Seven Categories of Enabling Security Technologies[138]

This research is an important element in support of the proposed recommendations because it shows that investing in network security can pay for itself and provide organizations with an overall net cost savings from cyber attacks. Showing that organizations can realize cost savings through network security practices, supports the recommendations for the DOD to influence stronger network security in third-party networks. The DOD's influence comes from showing third-party network owners net cost savings from employing stronger network security practices.

In research related to the cost of cyber attacks, some authors have also proposed theories on why many organizations do not invest more heavily in their network security. Their arguments claim that even while conservative estimates indicate the cost of cyber attacks is very substantial, it is still actually only a small percentage of many organizations' bottom lines. Hackett uses work done by Benjamin Dean, at Columbia University's School of International and Public Affairs, to show that costs associated

[138] Source: Ponemon Institute, "2015 Cost of Cyber Crime Study: Global," 20.

with cyber attacks usually amount to less than 1 percent of most companies' earnings, which correlates with work by other authors noted earlier.[139] However, when other things such as insurance payouts and tax write offs are considered, the actual cost to companies becomes even less.[140] Hackett uses the well-known Sony, Home Depot, and Target network breaches as examples to describe the actual scale of the costs associated with the attacks to the companies' overall bottom lines. He uses a quote from Sony's financial forecast, "Sony believes that the impact of the cyberattack on its consolidated results for the fiscal year ending March 31, 2015 will not be material."[141] Hackett also uses statistics from Dean that show, when mitigating factors such as insurance policies and tax breaks are figured in, the breaches at Home Depot and Target will represent approximately 0.01 percent and 0.1percent of their annual sales in 2014, respectively.[142] Organizations may feel these costs are less than the cost of investing in stronger security, especially when considering cost mitigating factors. Consequently, instead of correcting their poor security, many organizations choose to overlook it or use insurance in an attempt to mitigate the potential negative financial impacts that stem from it. Gandel notes that the insurance industry has seen insurance premiums collected on cyber policies grow from less than $1 billion to over $2.5 billion in just three years.[143] These actions may well prove short-sighted because, as already noted, there are many components to the costs of cyber attacks, all of which may not be readily apparent in cost estimates and company financial reports.

Regardless of the lack of hard estimates, people should intuitively recognize that the overall cost of cyber-attacks to the United States, in terms of governmental, corporate, and individual costs are enormous. Thwarting cyber-attacks through improved network

---

[139] Robert Hackett, "How Much do Data Breaches Actually Cost Big Companies," *Fortune.com*, April 1, 2015, http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/.

[140] Benjamin Dean, "Sorry Consumers, Companies Have Little Incentive to Invest in Better Cybersecurity," *Quartz*, March 05, 2015, http://qz.com/356274/cybersecurity-breaches-hurt-consumers-companies-not-so-much/.

[141] Ibid.

[142] Ibid.

[143] Gandel, "Lloyd's CEO: Cyber attacks Cost Companies $400 Billion Every Year."

security is a key element to reducing these costs. The information gathered from literature in this area provides evidence that the strategies to improve third-party network security will be cost effective for both the third-party network owners and the DOD.

G. SYSTEMS ENGINEERING APPROACH

Systems engineering is an important field in the modern world and in particular to the DOD. It is the engineering method society uses to create modern complex systems used for purposes in everyday life and modern warfare. However, a description and working definition of a "system" is essential to understanding systems engineering. The International Council on Systems Engineering (INCOSE) defines a system as:

> A "system" is a construct or collection of different elements that together produce results not obtainable by the elements alone. The elements, or parts, can include people, hardware, software, facilities, policies, and documents; that is, all things required to produce system-level results. The results include system-level qualities, properties, characteristics, functions, behavior, and performance. The value added by the system as a whole, beyond that contributed independently by the parts, is primarily created by the relationship among the parts; that is, how they are interconnected.[144]

Blanchard asserts that a system also has a number of general characteristics. These characteristics are a system is made of a combination of resources, falls into some sort of hierarchy, contains components and/or subsystems, and has a functional purpose.[145] To further describe systems, Blanchard breaks systems down into several different categories. The categories of systems he lists are natural and manmade, physical and conceptual, static and dynamic, closed-loop and open-loop.[146]

Systems can also be joined or integrated with other systems to form a relationship called a system-of-systems (SOS). Examples of SOS would be a transportation system, a large scale communications system, or a complex DOD weapon system, such as an aircraft carrier. Blanchard provides the following as the definition of a SOS:

---

[144] Blanchard, *System Engineering Management*, 3.

[145] Ibid., 3–4.

[146] Ibid., 4–5.

A collection of component systems that produce results unachievable by the individual systems alone. Each system in the SOS structure is likely to be operational in its own right, as well be contributing in the accomplishment of some higher-level mission requirement. The life cycles of the individual systems may vary somewhat as there will be additions and deletions at different times, as long as the mission requirements for any given system are met. Thus, there may be some new developments in progress at the same time as other elements are being retired for disposal.[147]

Blanchard, in Figure 7, provides a visual depiction of example SOSs:

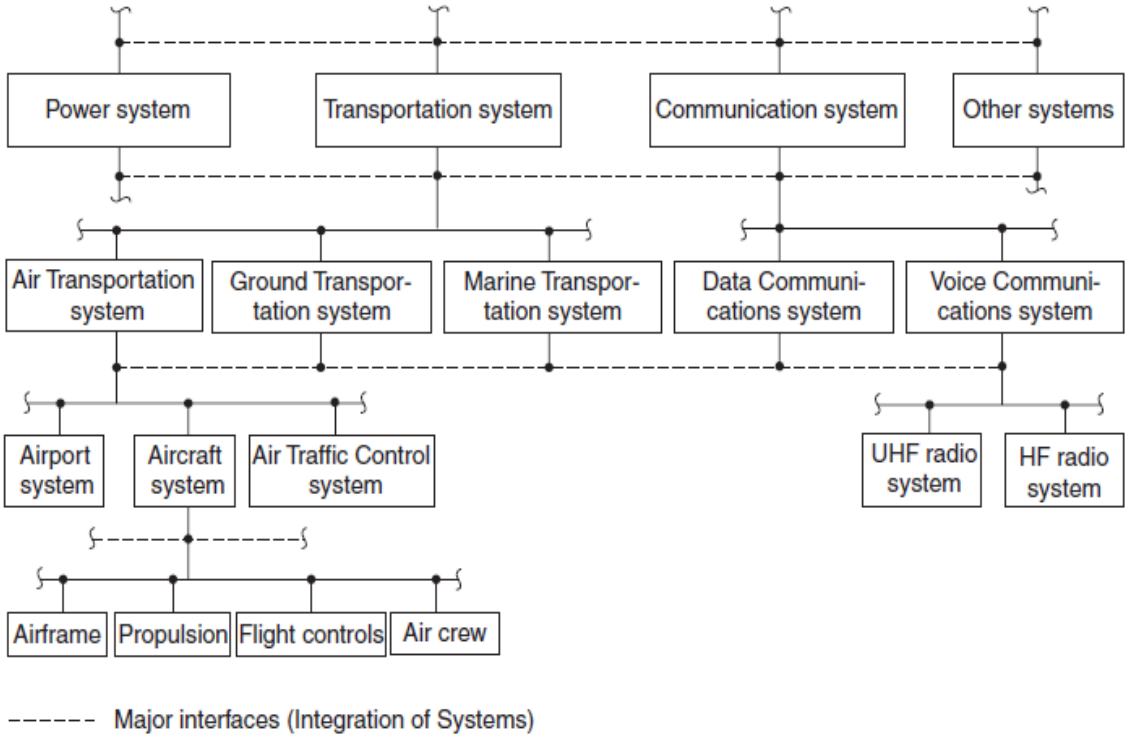


Figure 7. Multiple Systems (SOS)[148]

This understanding of a system and a SOS, allows the reader to grasp the systems engineering process. Several definitions of systems engineering are available. First, INCOSE has defined it as:

[147] Ibid., 7.

[148] Source: Ibid., 7.

> Systems engineering is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem. Systems engineering considers both the business and technical needs of all customers with the goal of providing a quality product that meets the user needs.[149]

The DOD has its own definition of systems engineering, provided by the *Defense Acquisition Guide Book*:

> Systems engineering (SE) is a methodical and disciplined approach for the specification, design, development, realization, technical management, operations, and retirement of a system. The enabling system elements provide the means for delivering a capability into service, keeping it in service, or ending its service and may include those processes or products necessary for developing, producing, testing, deploying, and sustaining the system.[150]

These definitions show that systems engineering cannot be thought of in the same manner as other hard engineering disciplines. Systems engineering is focused on the design and development processes required to bring a system from being simply a requirement to an actual functional system.[151] A critical component of good systems engineering is "a 'top-down/bottom-up' development approach"[152] that uses feedback loops at each stage that allow for continuous design, product, and process improvement.[153] This approach provides the "top down" direction from higher level leadership during the design and initial construction phases, as well as, bottom up refinement in product and process improvement during later phases. Figure 8 depicts this process with its associated feedback loops:

---

[149] Ibid., 17.

[150] Department of Defense, *Defense Acquisition Guidebook*, 158 (2013).

[151] Blanchard, *System Engineering Management*, 21.

[152] Ibid., 18.

[153] Ibid., 31.

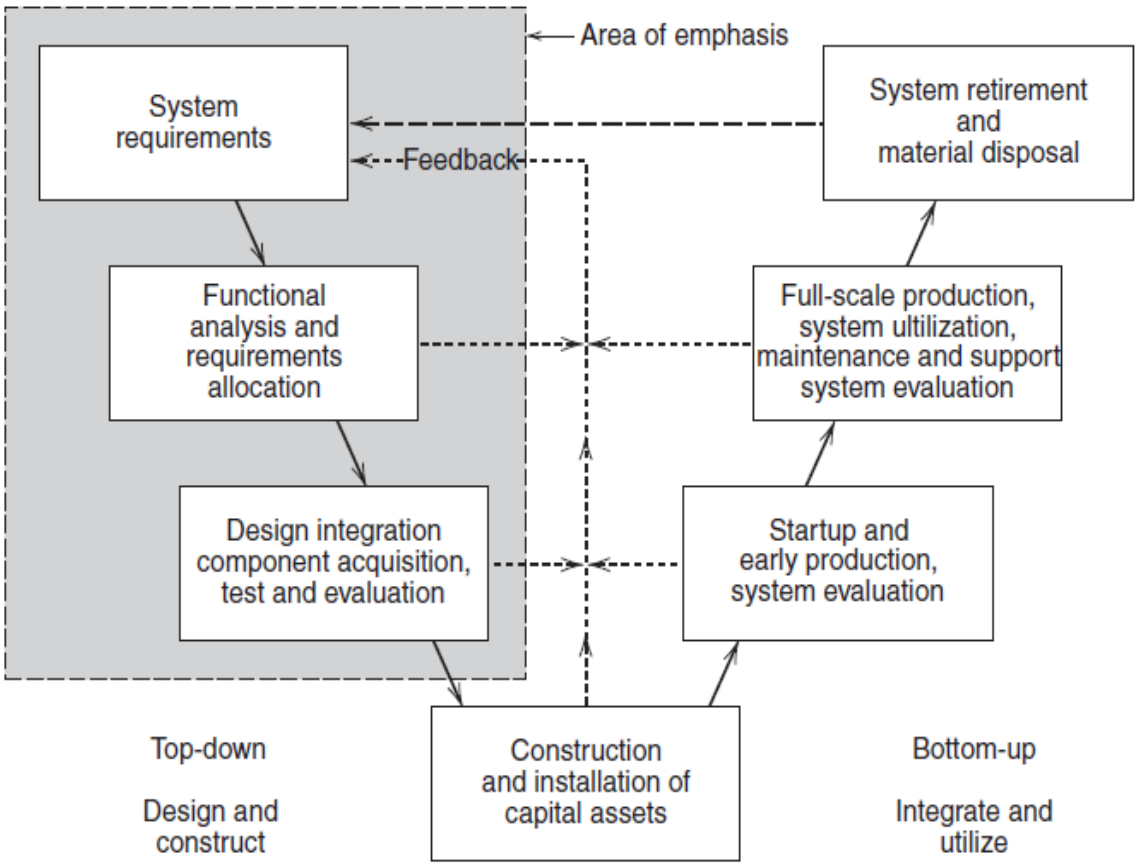


Figure 8. Top-Down/Bottom-Up System Development Process[154]

The systems engineering process should be applied through all phases of a system's life cycle. By doing this, systems can be continually assessed to provide feedback on recommendations for changes to the system in order to keep systems optimally functional.[155] Figure 9 shows how the systems engineering process should meld with the system life cycle:

[154] Source: Ibid., 19.

[155] Ibid., 51.

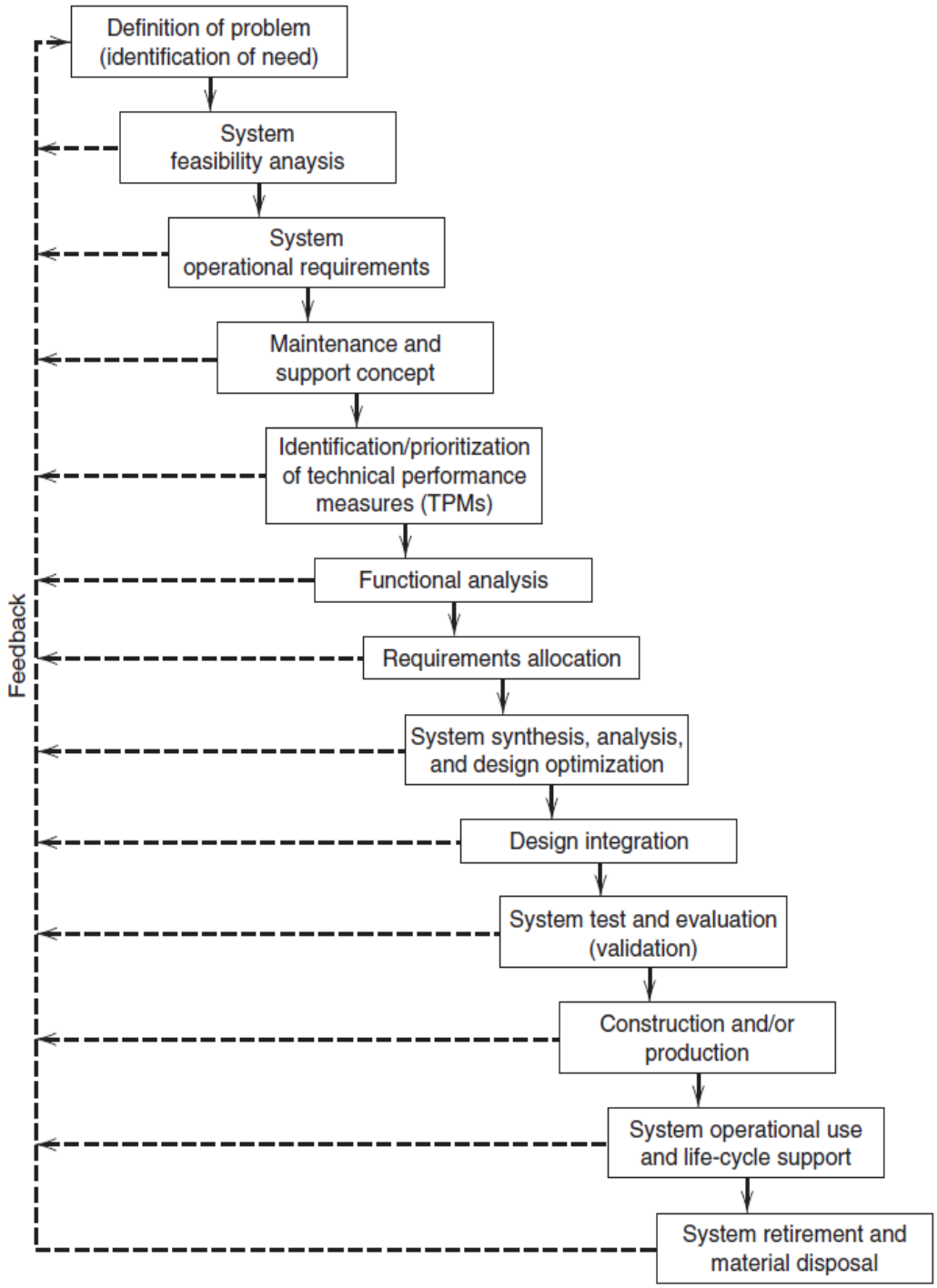


Figure 9. The System Engineering Process in the Life Cycle[156]

[156] Source: Ibid., 52.

In the modern technological world, and specifically in the DOD, many new systems will become part of an SOS. Few systems operate in a standalone fashion. Blanchard contends that one of the primary systems engineering objectives is to ensure leadership and provide guidance during the system design phase.[157] A critical design element is ensuring the system can effectively interface and is interoperable with other external systems as either part of an integrated SOS or as standalone systems operating in the same environment.[158] Figure 10 graphically depicts this system interoperability requirement:

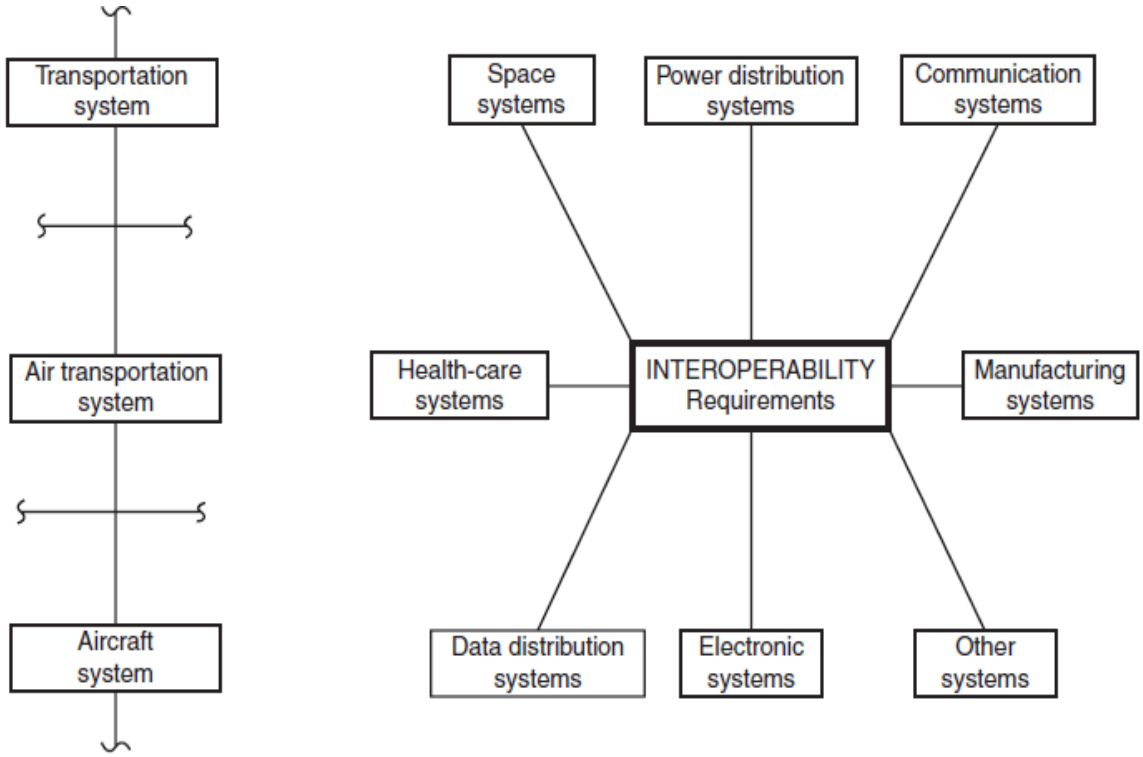


Figure 10. System-of-Systems Integration and Interoperability Requirements[159]

Good systems engineering practices become increasingly important as modern systems grow ever more complex and are integrated into more complex SOSs. This

[157] Ibid., 125.

[158] Ibid., 205–207.

[159] Source: Ibid., 211.

review provided important background information on the systems engineering methodology, which is used to develop the recommendations in this thesis. The recommended actions to influence improved security postures in third-party networks are viewed as individual systems. The systems engineering methodology will ensure the compatibility of the recommended actions within the larger DODIN SOS.

H. CONCLUSION

Third-party computer networks represent a risk to DOD computer networks. As the DOD is operationally reliant on its networks, third-party networks also represent a risk to DOD operations. The literature review indicates that the government is taking actions to mitigate these threats in several different ways. The DOD and DHS respective cyber threat information sharing and anti-terrorism technology programs and clauses in federal government acquisition regulations are the most applicable for the purposes of this thesis. These specific areas are analyzed in further detail in following chapters.

III. EXISTING FEDERAL GOVERNMENT PROGRAMS

A. INTRODUCTION

One of this chapter's objectives will be to demonstrate that precedence exists within the federal government that can be used to inform and strengthen this thesis's overall recommendations. These precedents are important to this work for several reasons, but most importantly they provide a model that can be used to structure recommended actions. Also, these precedents may increase the probability of the DOD implementing the recommended actions because they demonstrate similar actions have been taken in the past, thus the actions are feasible and a path to follow in implementing them has already been created. The literature review for this thesis, contained in Chapter II, demonstrates that precedence does exist in the form of two existing federal government programs: the DHS Safety Act Program and the DOD Cyber Security/ Information Assurance (CS/IA) Program. This chapter delves into the detailed aspects of the programs' governing policies, structures, and boundaries. It also highlights how portions of these two programs can be used as exemplars to design a program that meets the system requirements to address the DOD's operational need. This operational need is the ability to influence the security posture of third-party networks, which may contact or connect to the DODIN.

B. DHS SAFETY ACT PROGRAM

As a result of terror attacks on September 11, 2001, the Safety Act was enacted in conjunction with the Homeland Security Act of 2002.[160] The government believed that following the attacks, many companies were fearful that they could be held liable and face severe litigation if their products or services were employed in a civilian environment where damage to property and people occurred as a result of terror

[160] Department of Homeland Security, Science and Technology Directorate, Office of SAFETY Act Implementation, *SAFETY Act 101Briefing: The Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002*, 2, https://www.safetyact.gov/pages/homepages/Home.do.

attacks.[161] This fear of liability had the potential to stagnate critical anti-terrorism technology development. Thus, Congress wrote and approved the Safety Act to shield companies who were developing and deploying certain anti-terrorism technologies from at least a portion of that litigation risk. Ultimately, "the SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by creating a system of 'risk management' and a system of 'litigation management.'"[162]

The Code of Federal Regulations (CFR) provides the Safety Act's formal title: "The Support Anti-terrorism by Fostering Effective Technologies Act of 2002."[163] According to the Federal Register, the Safety Act's primary purpose is to "ensure that the threat of liability does not deter potential manufacturers or sellers of anti-terrorism technologies from developing, deploying, and commercializing technologies that could save lives."[164] The Act provides several different liability protections, such as exclusive jurisdiction in Federal Court for suits against sellers of a Qualified Anti-Terrorism Technology (QATT), limitation of the liability to the amount of terrorism insurance the seller is carrying, a limitation on the amount of non-economic damages, a total prohibition on punitive damages and any pre-judgment interest, a reduction in the award amount to the claimant by the amount of any other compensation received by the claimant, a presumption the seller is entitled to the 'government contractor's defense.'"[165] The government contractor's defense makes the seller immune from liability for claims where the Safety Act applies. Furthermore, the act ensures that any liability that does exist does not extend past the seller of the QATT. If litigation were brought against others in the supply chain of a QATT, the costs would ultimately trickle back to the seller and serve to suppress initiative in developing new QATTs. So the Act

---

[161] Department of Homeland Security, Science and Technology Directorate, *SAFETY Act Fact Sheet* (January 14, 2016), https://www.safetyact.gov/pages/homepages/Home.do.

[162] Regulations implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act), *Federal Register* 71, no. 110, 33148 (June 8, 2006).

[163] Regulations to Support Anti-Terrorism by Fostering Effective Technologies Code of Federal Regulations, 6 C.F.R. § 25 (January 1, 2014), 178, https://www.gpo.gov/fdsys/pkg/CFR-2014-title6-vol1/pdf/CFR-2014-title6-vol1-part25.pdf.

[164] Ibid

[165] Ibid.

prevents suits from being brought against suppliers to the QATT seller or QATT buyers and downstream users.[166] However, as DHS notes, the Safety Act protections only apply in the case of an actual terrorism event.[167]

Under the Safety Act, QATT sellers are required to obtain liability insurance for their approved technologies. The amount of liability insurance the QATT seller must obtain will be included in the QATT designation and certified by the Under Secretary for Science and Technology of the Department of Homeland Security.[168] Several factors are included in the determination of the actual amount of liability insurance the QATT seller must obtain, but in general, it is based on policies available on the insurance market, amounts that sellers of comparable products hold, and the amounts of insurance the seller held prior to the Safety Act Program application. However, the Under Secretary cannot require a seller to obtain any type or amount of insurance that is not available on the general insurance market or that would significantly skew the price of the seller's QATT.[169]

A wide range of products and services can be designated as a QATT and covered underneath the Safety Act. CFR defines a QATT as "any Technology (including information technology) designed, developed, modified, procured, or sold for the purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause."[170] Examples of technologies eligible to be covered by the Safety Act include threat and vulnerability assessment services, blast mitigation services, sensors, vaccines, metal detectors, data mining software, and many others.[171] Once any of these technologies are approved as a QATT, their sellers and buyers will

---

[166] Ibid., 33150-33151.

[167] Department of Homeland Security, Science and Technology Directorate, Office of SAFETY Act Implementation, *SAFETY Act 101Briefing: The Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002*, 2.

[168] Regulations to Support Anti-Terrorism by Fostering Effective Technologies Code of Federal Regulations, 6 C.F.R. § 25 (January 1, 2014) 182.

[169] Ibid., 182–183.

[170] Ibid., 179.

[171] Randel L. Zeller, *"Bridging Technology Capability Gaps" Opportunities with the Private Sector*, Department of Homeland Security, Science and Technology Directorate, Interagency Office, 36, http://www.dtic.mil/ndia/2011jointmissions/TuesdayZeller.pdf.

received liability protections if that QATT is involved in a designated terrorism event, including cyber terrorism.

The Safety Act Program's structure contains two principle levels of liability protection: Designation and Certification.[172] The Designation Level also contains a secondary level called Developmental Testing & Evaluation (DT&E) Designation.[173] Figure 11 provides a graphical depiction of the Safety Act Program's liability protection levels:

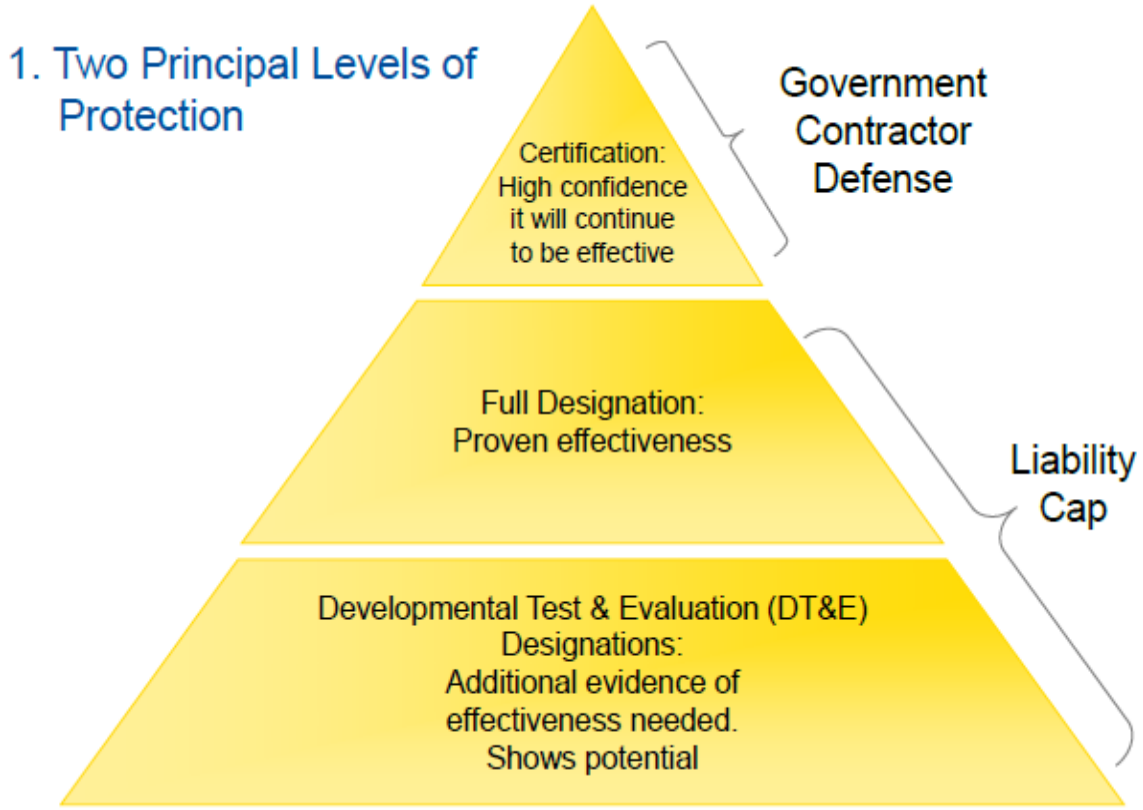


Figure 11. Safety Act Liability Levels[174]

[172] Department of Homeland Security, Science and Technology Directorate, Office of SAFETY Act Implementation, *SAFETY Act 101Briefing: The Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002*, 6.

[173] Ibid.

[174] Source: Ibid.

As described previously, the Designation Level provides the liability cap protections. Numerous criteria exist for a technology to qualify for the Designation Level: prior U.S. Government use or proven utility and effectiveness, the technology is available for immediate deployment, high probability the technology will not be deployed unless Safety Act protections are applied, magnitude of risk to the public if the technology is not used, and others.[175] The secondary DT&E Designation Level is for technologies that are in the testing phase and not ready for operational deployment. This subset receives the same protections as the Designation Level but only can be applied to testing and evaluation events at a limited number of locations.[176] The Certification Level is for technologies that have already qualified under the Designation Level and have also been demonstrated to perform as intended, shown to conform to the sellers' specifications, and proven safe for use in the manner and environments intended.[177] The Certification Level provides the same liability protections as the Designation Level, but also provides the government contractor defense against liability claims and puts the technology on the government's approved product list (APL) or approved services list (ASL).[178] Table 6 provides a summary of these liability protection levels:

[175] Ibid., 14.

[176] Ibid., 18.

[177] Ibid., 16.

[178] Ibid., 12.

Table 6. Safety Act Liability Protections Summary[179]

	DTED	Designation	Certification
Effectiveness Evaluation	Needs more proof, but potential exists	Proven effectiveness (with confidence of repeatability)	Consistently proven effectiveness (with high confidence of enduring effectiveness)
Protection	Liability cap only for identified test event(s) and for limited duration (≤3yrs)	Liability cap for any and all deployments made within 5 year term	Government Contractor Defense (GCD) for any and all deployments made within 5 year term

Since the Safety Act's enactment, it has been heavily utilized by private sector anti-terrorism technology producers. As of January 2016, DHS has qualified over 800 technologies under the Safety Act Program at the different levels.[180] Data suggests that private sector use in also increasing. In Fiscal Year (FY) 2015, 87 technologies received Safety Act protections compared to 65 in FY 2014.[181] Additionally, the QATTs added in FY 2015 alone represented approximately $7.5 billion in revenue to the companies involved.[182] This data indicates the Safety Act Program has been successful in providing effective incentives for the private sector to continue innovating and developing new anti-terrorism technologies.

[179] Source: Ibid., 19.

[180] Department of Homeland Security, Science and Technology Directorate, *SAFETY Act Fact Sheet*.

[181] Department of Homeland Security, Science and Technology Directorate, Office of SAFETY Act Implementation, *SAFETY Act Webinar: The SAFETY Act and Business: Protecting You and Informing Your Customers*, 2 (December 02, 2015), https://www.safetyact.gov/jsp/refdoc/samsRefDocSearch.do.

[182] Ibid.

C. DOD DIB CS/IA PROGRAM

The DOD initially established the Defense Industrial Base (DIB) Cyber Security/ Information Assurance (CS/IA) Program in 2007 under the DOD Chief Information Officer (CIO),[183] and in October 2013 made it a permanent program within the DOD.[184] The program is governed by DOD Instruction, Number 5205.13.[185] The DOD established the program because it recognized that cyber threats to unclassified networks within the DIB represented a severe risk to DOD information and ultimately national security. According to the CFR, the program's purpose is to "enhance and supplement DIB participants' capabilities to safeguard DOD information that resides on, or transits DIB unclassified information systems."[186] So the program's primary focus is on DOD CUI and UCTI that contacts DIB networks.

Overall, the DIB CS/IA Program contains several different elements that contribute to accomplishing the program's purpose. It shares DOD unclassified and classified cyber threat information, as well as, computer network defense (CND) and IA best practices with DIB participants. The program develops standard reporting procedures for DIB cyber incident reporting and develops mechanisms for the DOD to assist the DIB participants in conducting cyber security self-assessments. It also develops procedures for the DOD to assist DIB participants in cyber attack damage assessments and network remediation.[187]

However, at its core, the DIB CS/IA Program is centered on information sharing. It utilizes bilateral information sharing, where the DOD provides the DIB program participants with information on current cyber threats and IA best practices to enhance

---

[183] Department of Defense, *DOD's DIB CS/IA Program: A Public-Private Cyber Security Partnership*, 2 (April 22, 2014), http://www.dtic.mil/ndia/2014cyber/Michetti.pdf.

[184] Department of Defense, *DIB Cybersecurity Activities Fact Sheet: DOD – DIB Cybersecurity Information Sharing Program Overview*, (October 6, 2015), http://dodcio.defense.gov/.

[185] Assistant Secretary of Defense (NII), *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*, DOD Instruction 5205.13, 1.

[186] Department of Defense (DOD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 32 C.F.R. § 236 (July 1, 2013) 551, https://www.gpo.gov/fdsys/ granule/CFR-2013-title32-vol2/CFR-2013-title32-vol2-part236.

[187] Assistant Secretary of Defense (NII), *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*, DOD Instruction 5205.13, 2.

their ability to protect DOD CUI and UCTI. In return, the participating companies provide the DOD with reports on certain cyber intrusions into their networks.[188] This information sharing arrangement is formalized in a standardized, bilateral framework agreement (FA), which is signed by both the DIB participant and the DOD, thereby legally implementing the agreement's requirements.[189] The program is entirely voluntary for DIB participants,[190] and the FA can be cancelled at any time, by either the DIB participant or the DOD. The DOD also recognizes a critical element in the success of this program is the sensitive nature of the information being shared by both the DIB participants and the DOD, and the importance of protecting that information from unauthorized use or disclosure.[191]

The DOD has created a DIB Collaborative Information Sharing Environment (DCISE), which is the operational hub for the DIB CS/IA Program's information sharing. The DCISE is operationally controlled through the DOD cyber crime center (DC3), which hosts the DCISE on a website: http://dibnet.dod.mil/.[192] This is how the DOD promulgates information on the program, handles applications, facilitates the bilateral information exchange of unclassified and classified threat information, and analyzes attacks to assist developing mitigation strategies in near real time with the DIB participants.[193] The DOD has also set up the DIB CS/IA Program Office to be the overarching point of contact for the program.[194]

To be eligible to participate in the DIB CS/IA Program, a DIB company must meet several requirements. Companies must have DOD-approved medium assurance

---

[188] Department of Defense (DOD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, *Federal Register* 77, no. 92, 27616 (May 11, 2012).

[189] Ibid.

[190] Ibid.

[191] Ibid.

[192] Department of Defense (DOD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 32 C.F.R. § 236 (July 1, 2013) 553.

[193] Department of Defense, *DIB Cybersecurity Activities Fact Sheet: DOD – DIB Cybersecurity Information Sharing Program Overview.*

[194] Department of Defense (DOD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 32 C.F.R. § 236 (July 1, 2013) 553.

certificates to allow encrypted unclassified information sharing, have an existing active Facility Security Clearance (FCL) approved for classified information if they are to receive it, have a communication security (COMSEC) account, and have access to the DOD's secure voice and data transmission systems. Additionally, the companies must own or operate a covered DIB system. Lastly, they must execute an FA with the DOD.[195]

As the DIB CS/IA Program is voluntary, the DIB participant is in no way obligated to use the information shared by the government. Consequently, any action the participant takes is their own decision to do so, and they are responsible for any costs associated with those actions.[196] These costs can include those associated with identifying, analyzing, and reporting cyber incidents, as well as costs to remediate the participant's network.[197] Additionally, being a voluntary participant in the program does not provide the company with any additional financial incentives or any special advantage competing for government contracts. In fact, Title 32 of the CFR directly states that the current program does not offer any contracting advantage for participating DIB companies.[198]

D. ANALYSIS

The DOD CS/IA Program's current elements work to enhance network security and provide some small amount of incentive for DIB companies to join the program. These elements are both useful and important, and they should remain as part of any new proposed program. However, the DOD could make the program much more effective by making several changes to it. First, the program's scope is too narrow. The program currently only includes DIB companies that have covered networks that contain or pass CUI and UCTI.[199] It should be broadened so it is open to any companies whose networks

---

[195] Ibid., 556.

[196] Ibid., 555.

[197] Department of Defense (DOD)-Defense Industrial Base (DIB) Cybersecurity (CS) Activities, *Federal Register* 80, no. 191, 59582 (October 2, 2015).

[198] Department of Defense (DOD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 32 C.F.R. § 236 (July 1, 2013) 555.

[199] Ibid., 551 & 556.

interact with the DODIN or that handle operationally relevant DOD information. Second, the program should be restructured to incorporate more incentive for DIB companies to both join the program and improve the security posture of their networks. The DOD should restructure the DOD DIB CS/IA Program to a layered or tiered structure and incorporate additional elements similar to those in the Safety Act Program, such as liability protections, adding products to approved purchase lists, and giving program participants added weight in contract bidding evaluations could increase the incentive for DIB companies to join.

Since the Safety Act Program already contains these elements, it serves as a model for how to modify the DOD DIB CS/IA Program. Adding liability protections to the DOD DIB CS/IA Program would almost certainly require legislative action to codify those protections into law. However, since legislative action was taken for the Safety Act to promote anti-terrorism technologies, it could also be taken for the DOD DIB CS/IA Program to promote cyber security. Additionally, the Federal Government and DOD have the ability to add the products of program participants to approved purchase lists and give added weight to contract bids from program participants during the bid evaluation process.

E. SUMMARY

The DOD DIB CS/IA Program was a starting point for the DOD to reach out to and assist the private sector in improving its network security. Information sharing on current threats, incident reporting, network security assessment assistance, threat mitigation assistance, damage assessment assistance, and network remediation assistance are all valuable tools in influencing the network security of these private organizations. However, the application of the program is too narrow. Thus, presently, the DIB CS/IA Program does not have the capability to influence all private sector third-party networks that contact some part of the DODIN. Many material and service providers for the DOD would not qualify for the program, yet their networks still contact the DODIN in some way. That contact is all that is required to provide an attack vector to an adversary.

Additionally, the DOD DIB CS/IA Program could do more to further incentivize improved network security of private sector third-party networks. The literature review provided evidence that companies are already recognizing the litigation risk they face due to network security breaches. The Safety Act Program's liability protections, APLs, and ASLs provide a powerful incentive to join the program. Many companies can gain a substantial advantage in their market when their products and services can legally short cut through the normal governmental contracting and acquisition process. As noted previously, current data suggests these incentives work, as over 800 companies have joined the Safety Act Program since its inception.

Overall, the DOD DIB CS/IA Program can be made much more effective at influencing the security of private sector third-party networks by retaining its current elements and also broadening its scope to incorporate certain Safety Act Program elements and other non-Safety Act related elements. This thesis's next chapter will serve to specifically analyze the elements that should be incorporated into the DIB CS/IA Program to improve its effectiveness.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS OF PROPOSED MODIFICATIONS TO THE DOD DIB CS/IA PROGRAM

A. OVERVIEW

The DOD DIB CS/IA Program can be significantly enhanced by restructuring it into a two-tiered, incentive-based information network security program. This restructured program is called the Enhanced DOD CS/IA Program. Each tier in this program contains different levels of security requirements and incentive elements for participants. Its proposed structure will prove crucial to incentivize improved information network security posture within the DIB. The enhanced program improves DIB network security by convincing DIB participants to voluntarily agree to meet the program's network security requirements in exchange for incentive elements that provide financial benefits and DOD assistance in improving their network security. Improved network security within the DIB reduces the threat vectors into the DODIN, thereby improving the DODIN's overall security and reducing its operational risk.

The DOD states that it expects up to 10 percent of the 8,500 covered defense contractors could ultimately join the current program, but actual program enrollment is currently less than half of that amount.[200] This low percentage of participants plus the current program eligibility requirements limiting potential participants demonstrates a shortcoming of the current program's design. Conversely, as discussed in Chapter III, the DHS Safety Act Program has demonstrated the ability of a government, incentive-based program to shape the actions of private companies in ways that benefit anti-terrorism activities. The Safety Act Program also clearly demonstrates the ability to generate interest and attract participants as indicated by the more than 800 technologies already approved for enrollment and data showing that application and approval rates are also increasing. While directly comparing these two programs is of arguable value, an indirect comparison indicates the more incentivized Safety Act Program is generating more participation, thus influencing more actions. Consequently, the Safety Act Program's

[200] Department of Defense (DOD)-Defense Industrial Base (DIB) Cybersecurity (CS) Activities, *Federal Register* 80, no 191, 59584 (October 2, 2015).

incentive based success provides evidence that a more powerful incentive based DIB CS/IA Program could reach more companies and better shape their actions to improve network security. Thus, the Safety Act Program is used as the model for the Enhanced DOD CS/IA Program's proposed structure.

B. PROPOSED DOD CS/IA PROGRAM STRUCTURE

The enhanced program contains two tiers: basic and advanced. These two tiers include differing levels of incentives and network security requirements. The enhanced DOD CS/IA Program has two tiers as an optimized solution between flexibility for the participants and simplicity in program structure. Going back to the Safety Act Program as the model, it utilizes two primary levels with a sub-level underneath its base level. This structure has proven successful in attracting companies to the Safety Act Program initially, and then incentivizing them to move to the higher level. The Safety Act Program Office acknowledges companies enter the program at the lower Designation Level to receive the basic level of protections, with some willing to move up to the Certification Level to receive its increased protections and benefits. This two-level system seems to provide participants with enough flexibility to make the program work to their benefit without creating undue complexity.

One key aspect of the original DIB CS/IA Program will remain unchanged—it will remain completely voluntary. Program participants will be free to withdraw from the program at any time. The DOD cannot mandate that private companies join or remain a part of a DOD-run program, especially one that could have financial implications for those companies. Thus, the enhanced program must remain voluntary. DIB companies are also free to choose the program tier that is the best fit for their organization and are also free to change tiers in order to find that best fit. The DOD can encourage and assist participants to reach the advanced tier to achieve its enhanced network security benefits, but the DOD should not pressure participants to join the advanced tier if they otherwise would not choose to do so. Doing so would go against the program's voluntary nature.

1. The Basic Tier

The basic tier will be the initial entry level into the DOD DIB CS/IA Program. Participants at this tier will be required to adopt basic security practices already required of DIB companies that deal in CUI and UCTI and have contracts with the DOD. As previously noted in Chapter II, the DOD must follow DFARS Clause 252.204-7012 when contracting with DIB companies.[201] This DFARS Clause mandates companies abide by network security practices set forth in NIST SP 800–53: "Security and Privacy Controls for Federal Information Systems and Organizations."[202] As also noted in Chapter II, forthcoming changes to the FAR will also require DIB companies to abide by security practices outlined in NIST SP 800–171: "Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations."[203] Since the network security practices contained in these two NIST publications are or soon will be required for DIB companies dealing in CUI and UCTI, it makes logical sense to set these the security practices as the requirements for the basic tier. Lastly, network security configuration practices set forth in NIST SP 800–70: "Security Configuration Checklists for IT Products" will also be used to set security requirements for the basic tier. Setting the NIST practices as requirements for the enhanced program is one of the crucial changes that will improve network security in the DIB participants' networks. Additionally, the basic tier will also retain the reporting requirements from the participant to the DOD as contained in the original program and required in the DFARS and FAR. This leads to another critical change to the enhanced program—validation that program participants are meeting the program's network security and reporting requirements.

The enhanced program's validation requirement comes in the form of a network security self-assessment the participants must complete, certify, and return to the DOD. To facilitate this self-assessment, the DOD will create a form or checklist that is based on

---

[201] Department of Defense, Defense Federal Acquisition Regulations Supplement, Clause 252.204-7012. *Safeguarding of Unclassified Controlled Technical Information*. (November 2013). http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm.

[202] Ibid

[203] Office of Management and Budget. *Improving Cybersecurity Protections in Federal Acquisitions*. (n.d.). https://policy.cio.gov/.

the previously mentioned NIST special publications and the reporting requirements from the FAR, DFARS, and the current DIB CS/IA program. Appendix B provides an example of how this self-assessment form might be constructed and the security controls it should contain. When DIB companies apply for the program, part of the application process is to use this self-assessment form to guide them through the self-assessment process. The DOD will provide technical assistance in using the enhanced program's self-assessment form and completing the self-assessment if requested by the applicants. As discussed previously, the current DOD DIB CS/IA Program is authorized to provide some assistance to DIB participants in conducting network security self-assessments.[204] Thus, the authorization to provide assistance in using this self-assessment form already exists. In the enhanced program, this assistance will be provided through the program office by trained and specifically-designated personnel. The assistance will consist of answering questions about what the security control items on the form specifically mean, how to procedurally complete the form, and recommendations on how to apply the form to the applicants' specific networks. Upon completion of the self-assessment, the applying companies will certify its completion and that their networks meet the security standards set in the assessment form. If areas exist in which their networks do not meet these security standards, the companies must also submit corrective action plans to the DOD with the certified self-assessments as part of their applications. Companies will be required to certify the substandard aspects of their networks have been corrected before the application process is finalized. If network intrusions are discovered during the self-assessment, the application process will halt until the applicants remediate their networks. The applicants are responsible for this network remediation cost.

To guard against applicant companies misrepresenting themselves on the network security self-assessments, the enhanced program will allow the DOD to spot check participant companies to verify the accuracy of their submitted assessment forms. The DOD can choose to do the self-assessment verification via organic DOD capability or contracted service. The DOD will be responsible for bearing the cost of the self-

[204] Assistant Secretary of Defense (NII), *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*, DOD Instruction 5205.13, 2.

assessment verification. Additionally, as part of the enhanced program, the DOD will specifically verify the accuracy of the self-assessment form of any networks that sustain a verified breach, which affects DOD information or the DODIN. If the program participants are found to have misrepresented themselves on the assessment or failed to maintain the required network security standards following the assessment, the DOD can decide to drop them from the program. Also, if the situation warrants, the DOD could decide to take further action against the participants, such as barring them from receiving future DOD contracts. Lastly, the network security self-assessment will be an annual requirement for participants to remain an active member of the Enhanced DOD CS/IA Program's basic tier. The NIST SP 800–115: "Technical Guide to Information Security Testing and Assessment," recommends that an organization's network assessment policy be reviewed annually,[205] and completing an annual self-assessment falls in line with this NIST best practice.

The incentive for DIB companies to join the program at the basic tier will come from several different program elements. First, the original program's core element, the bilateral information sharing on current cyber threats in real time will remain at this tier. The information sharing will continue to be processed through the DCISE, which will continue to be hosted by the DC3. As with the current program, DIB participants will be able to receive classified threat information if they are cleared and certified to receive and store classified information. This program element will allow the DOD to keep the DIB participants updated on the current cyber threats the DOD tracks so the participants can better prepare their networks to defend against those threats. So this program element provides a free cyber threat intelligence source for the DIB participants.

Secondly, the enhanced program will provide continued assistance to participants who wish to conduct vulnerability assessments on their own networks. To do this, the program will offer a repository of leading network and vulnerability scanners: Nessus, SuperScan, NMap, NetClarity, Retina, and others. Many of these scanners are freeware,

---

[205] National Institute of Standards and Technology, *Special Publication 800–115: Technical Guide to Information Security Testing and Assessment*, 6–1 (September 2008), http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

but a few such, as the Nessus[206] and Retina[207] scanners, must be purchased. Through the program, the DOD will offer the scanners to the enhanced program participants. The freeware scanners can be downloaded directly from the Internet. The DOD can purchase licenses for the scanners that are not freeware and then provide those licenses to program participants. Tenable, who produces the Nessus scanner, and Beyond Trust, who produces the Retina scanner, sell blocks of product licenses. As a separate option, the DOD can work with companies providing the scanner licenses, in order to offer the licenses at a discounted rate to the program participants. Through the program office, the DOD will also provide technical assistance to the participants on using these tools. The assistance will include instructions on how to use the tools, recommendations on how to apply the tools to participants' networks, and limited trouble shooting advice.

Third, the DOD makes participation in the Enhanced DOD CS/IA Program an evaluation criterion used in the bid evaluation process for DOD contracts. This program participation criterion will not be a mandatory criterion for a company to be awarded a DOD contract, but merely garners participants increased consideration of their contract bids. Participants earn this increased contract bid consideration because through program participation they demonstrate to the DOD that they maintain a known, minimum level of network security vice non-participants whose network security level is unknown. This known security level reduces risk to the DOD. Thus, being an Enhanced DOD CS/IA Program participant could offer companies a competitive advantage over competitors when bidding on government contracts. In turn, this competitive advantage acts as an incentive to draw companies into program participation.

Lastly, the enhanced program's liability cap protection is the only program element that requires support from outside the DOD. Specifically, the DOD has no authority to set liability caps, so Congress will have to pass legislation to enact this portion of the enhanced program. However, doing so provides a significant incentive for

---

[206] "Nessus Professional," Tenable Network Security, accessed March 29, 2016, https://store.tenable.com/index.php?main_page=product_info&cPath=1&products_id=94.

[207] "Retina Network Security Scanner," BeyondTrust, accessed March 29, 2016, http://shop.beyondtrust.com/ store?SiteID=eeyeinc&Action=DisplayProductDetailsPage&productID=285899100&pgm=94163000.

DIB companies to join the Enhanced DOD CS/IA Program and adopt its improved network security practices. As discussed in Chapter II, organizations are paying rapidly increasing insurance premium costs, which indicate they see litigation resulting from cyber attacks as a significant financial threat. The liability cap protections in the enhanced program will be closely modeled after the liability caps on anti-terrorism technologies in the Safety Act Program. Consequentially, the Enhanced DOD CS/IA Program participants' legal liability will be capped at an amount equal the maximum amount of cyber attack insurance the participants are carrying. As with the Safety Act Program, the participants in this restructured DOD program will be required to carry a certain amount of insurance. The amount the participants are required to carry will be determined on a case-by-case basis and based on numerous factors. The two most critical factors are 1) to avoid artificially inflating the price of the participants' goods and services by setting the required policy amounts too high and, 2) to align the required policy amount with policies comparable organizations are taking out on the open insurance market. Ultimately, the DOD will set the policy amount each participant will be required to carry based on the evaluation of all the relevant factors. This determination will take place during the enhanced program application process, and stated clearly in the final agreement signed by both parties. This liability cap protection will only apply to claims made by third parties affected by cyber attacks targeted at the participants' networks due to their relationship with the DOD.

2. The Advanced Tier

The advanced tier represents the higher level of the Enhanced DOD CS/IA Program in terms of the level of network security requirements the participants must meet and the incentives offered through its program elements. To apply for the advanced tier, program participants are required to have already applied for and been found qualified to participate at the basic tier. Consequentially, advanced tier participants are required to meet the basic tier network security requirements and will receive the basic tier incentive elements while participating in the advanced tier. The advanced tier then incorporates more advanced network security practices into the program while also providing additional incentive elements.

DIB companies that desire to participate in the DOD DIB CS/IA Program's advanced tier are required to have a qualified independent third party conduct security assessments on their networks. These third-party assessments of the DIB companies' networks are accomplished via two avenues. First, the applicants must have an independent third party validate the network security self-assessment completed for the basic tier application. Second, the applicants are required to have the independent third party conduct thorough network vulnerability assessments and penetration testing on their networks in accordance with NIST SP 800–115: "Technical Guide to Information Security Testing and Assessment." The applicants are also required to submit a corrective action plan, which addresses vulnerabilities discovered during the vulnerability assessment process and the anticipated timeline to correct or mitigate those vulnerabilities in order to finalize the application process. The applicants will remain in an initial probationary status until they confirm to the DOD the vulnerabilities have been corrected, mitigated, or otherwise appropriately addressed in accordance with their corrective action plan. The applicants are also responsible for any costs associated with correcting the vulnerabilities on their networks. For DIB participants to remain enrolled in the advanced tier, they are required to periodically repeat network vulnerability assessments and penetration testing events. The author recommends the DOD set the period for periodic reassessments within the range of two to four years. A period set too short both creates an overly onerous and costly requirement, which may discourage participants. A period set too long allows for too much potential degradation in the network security posture. Current best practice guidelines do not set any specific frequency for network vulnerability reassessments. The NIST SP 800–53 states the frequency for vulnerability assessments and penetration testing is user defined,[208] and the Center for Internet Security (CIS) Critical Security Controls for Cyber Defense states that penetration testing frequency should be "regular."[209] Any network breach or intrusion that is discovered during the third-party assessment process halts the participants'

[208] National Institute of Standards and Technology, *Special Publication 800–53 revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*, F-62 and F-153 (April 2013), http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[209] Center for Internet Security, *The CIS Critical Security Controls for Effective Cyber Defense Version 6.0*, 69 (October 15, 2015), https://www.cisecurity.org/critical-controls.cfm.

advanced tier application process and causes the participants to be suspended from the program until the intrusion is remediated. The participants' are responsible for any network remediation costs.

The elements that create incentive for the enhanced program at the advanced tier build on those elements found in the basic tier. First, the DOD will offer to share the costs for the network vulnerability assessments and penetration testing to help ease the DIB participants' burden for these requirements. Numerous options exist to implement this incentive element. As examples, the DOD can set a flat rate cost percentage for all participants, set a cost ceiling the DOD will not exceed, or create a sliding scale percentage based on the participants' annual profit levels. Easing the participants' out of pocket cost burden for the assessments will increase the likelihood that DIB companies will decide to participate in the Enhanced DOD CS/IA Program at the advanced tier.

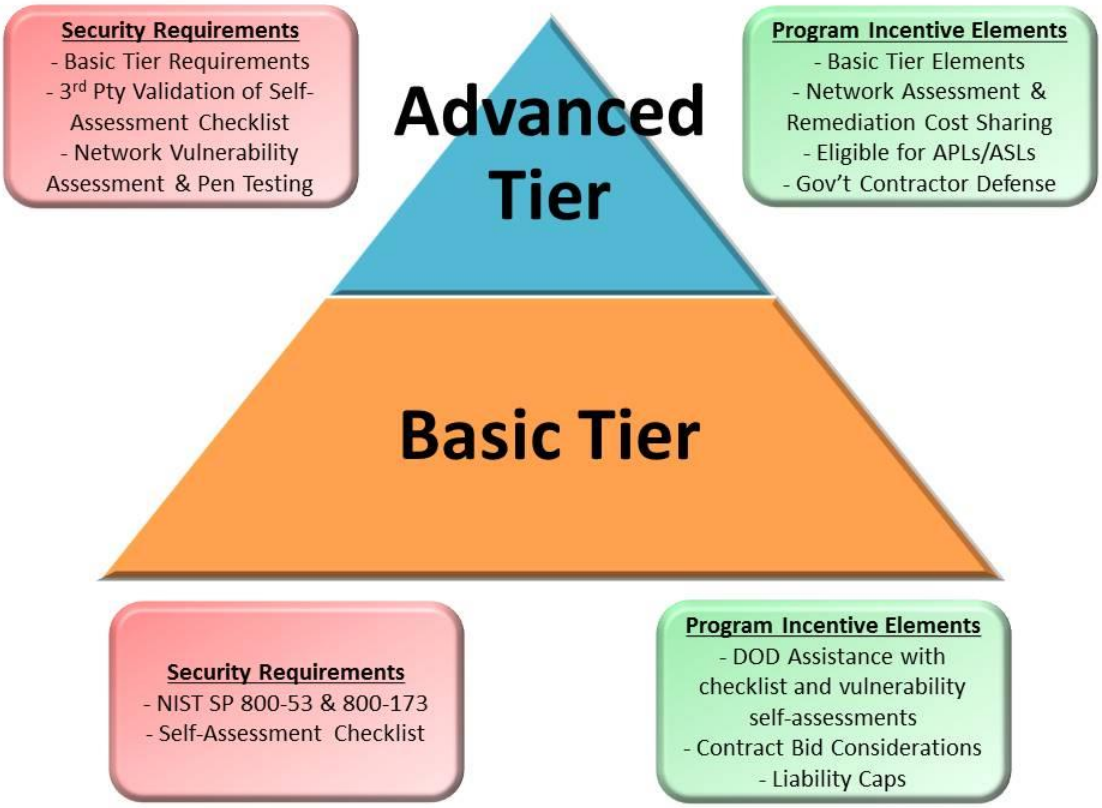
The advanced tier's second incentive element is DOD provided network remediation assistance for participants whose networks are breached by cyber attacks. As noted in Chapter III, the current DOD DIB CS/IA Program already contains provisions to provide technical remediation assistance to participants whose networks have been breached, and this will continue in the enhanced program. The technical capacity to effectively enable this incentive element could be created and reside organically within the DOD in either the DC3 or the DIB CS/IA Program Office, or it could be a contracted service. Additionally, in cases where attacks are determined to be directly linked to the program participants' relationship with the DOD, the enhanced program can also offer to share network remediation costs with the participants. However, the DOD will ensure that the participants are compliant in all aspects of the enhanced program prior to fulfilling this element and sharing any remediation costs. The DOD can choose to implement the network remediation cost sharing in a variety of ways. This cost sharing will serve to provide important assistance to the DIB participants, and also greatly strengthen the relationship between the participants and the DOD.

The creation of APLs and ASLs for DIB participants is the next element incorporated into the advanced tier. As discussed in Chapter III, within the Safety Act Program, the APLs and ASLs are preapproved purchase lists for products and services.

DIB companies who have joined at the advanced tier can have certain products or services placed on these preapproved purchase lists so that organizations within the DOD can purchase them without having to go through the full DOD contracting process. The DOD will have to set criteria on what types of products and services could legally be placed on these lists. However, for the companies that could have products and services placed on the APLs and ASLs, this program element could result in a significant market advantage over competitors and thus be a strong incentive for the program. As with the Safety Act Program, these APLs and ASLs could potentially be extended beyond the DOD and also applied to other federal government agencies, thereby magnifying this element's overall incentive effect.

The last program element in the advanced tier is to further strengthen the liability protections for the participants. This element is again modeled after the Safety Act Program in that, at this tier, program participants could be eligible for the government contractor defense in litigation proceedings. Eligibility for the government contractor defense gives the program participants liability immunity from third-party claims resulting from cyber attacks that caused network breaches. Eligibility for this liability protection, however, does not eliminate the basic tier requirement for the participants to hold a cyber attack insurance policy, but could prevent them from having to use it. As with the liability caps in the basic tier, this protection only applies to cyber attacks that are determined to be linked to the participants' relationship with the DOD. In the face of growing cyber attack litigation costs, this type of liability protection will serve as a very powerful incentive for DIB companies to join the program at the advanced tier and adopt its network security practices.

Figure 12 presents a visual depiction of the Enhanced DOD CS/IA Program including its security requirements and incentive elements:



The width of each tier represents the relative number of expected participants at that tier.

Figure 12. The Enhanced DOD CS/IA Program Structure

C. ENHANCED DOD CS/IA PROGRAM ADMINISTRATION

The structure to effectively administer the Enhanced DOD CS/IA Program already exists within the DOD. As previously discussed, the DC3, by hosting the DCISE, continues to operate the enhanced program's real time information sharing and cyber threat tracking component. So this part of the enhanced program's administrative structure requires little change. The current DOD DIB CS/IA Program Office also already exists. Since the program office is already in place, it is a reasonable initial location to handle all the remaining administration for the enhanced program. However, the program office must be structured and staffed to deal with all aspects program advocacy; application processing; providing technical assistance with network vulnerability self-assessments and network remediation; validation of network

vulnerability self-assessments; providing guidance and assistance for third-party conducted vulnerability assessments; coordinating with the DC3 to ensure active program participants have access to the DCISE; and coordination with the office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD AT&L) for establishment and maintenance of APLs and ASLs. The program office must also maintain and provide program participants the documentation required to invoke liability protections during litigation proceedings and deal with the enhanced program's cost sharing initiatives. The program office may require additional personnel structure and funding to effectively operate under the enhanced program's increased scope and administrative requirements. Since the baseline organizational structure for the enhanced program already exists, this increase in administrative requirements is not an insurmountable problem. Additionally, the DOD could decide to contract some of these administrative requirements, thereby reducing the administrative burden on the program office.

D. THE ENHANCED PROGRAM'S ASSOCIATED COSTS

The DOD will be required to bear some financial burden in order to establish and operate the Enhanced DOD CS/IA Program. At the basic tier, one program element is a cost driver: license costs for the vulnerability scanners that must be purchased. The DOD should work with the scanner providers to purchase the scanner licenses in bulk to reduce costs. The advanced tier has two program elements that are cost drivers: cost sharing for participants' post-breach network remediation and cost sharing for third-party conducted network vulnerability assessments and penetration testing. Any additional personnel overhead within the Enhanced DOD CS/IA Program Office is an additional cost driver for the program. To deal with the increased administrative burden of the enhanced program, at least some personnel structure may have to be added to the program office. The amount and type of personnel structure added is dependent on how the DOD implements the program and if the entire administrative burden described previously is placed directly under the program office, spread loaded among separate DOD offices, or potentially partially contracted out. In order to gauge the personnel costs, the author used the General Schedule (GS) pay scale. The GS grades listed in Table 7 were chosen as an

example set, as these grades are capable of handling the additional administrative tasks for the enhanced program. The companies listed under the scanner licensing and vulnerability assessment costs provided the cost information either through posted website information or through direct price quotes to the author.

Table 7 represents a summary of the costs from the Enhanced DOD CS/IA Program the DOD can expect to bear. The cost amounts listed in Table 7 will be affected by how the DOD ultimately decides to implement the enhanced program. So capturing exact costs at this point in the program design process is not feasible. Thus, the costs listed in Table 7 are meant to represent a rough order of the magnitude the DOD can expect to see for the enhanced program. Table 7 indicates the enhanced program's costs could be significant:

Table 7. Summary of Enhanced Program Costs to DOD

Personnel Costs[210]				
GS-5	GS-6	GS-7	GS-8	GS-9
$32,030	$35,704	$39,677	$43,939	$48,531

Basic Tier Costs			
Nessus & Retina Licenses			
Annual Nessus Manager License (128 host) Through Tenable[211]	Annual Nessus License Through Blue Tech Inc.[212]	Block of 500 Nessus Licenses Through Convergence Technology[213]	Annual Retina License Through Beyond Trust[214]
$2,920	$1,947	$1,578,890	$1,700

Advanced Tier Costs

[210] Office of Personnel Management, *2016 General Schedule (Base) Salary Table (Annual Rate)*, 2016, https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2016/general-schedule/.

[211] "Tenable Store," Tenable.com, accessed April 28, 2016, https://store.tenable.com/?main_page=index&cPath=23.

[212] Carly Evers (sales representative at Blue Tech Inc.), provided open market quote to the author, March 30, 2016.

[213] Darrell Boyd (sales representative at Convergence Technology), provided open market quote to the author, May 4, 2016.

[214] "BeyondTrust Store," BeyondTrust.com, accessed March 30, 2016, http://shop.beyondtrust.com/store?SiteID=eeyeinc&Action=DisplayProductDetailsPage&productID=285899100&pgm=94163000.

Network Vulnerability Assessments and Penetration Testing Costs			
Main Nerve		Convergence Technology	Core Security
10 External & 30 Internal IPs[215]	For a Larger Number of IP Bundles[216]	10 External & 150 Internal IPs[217]	Cost Per Week[218]
$1,299	$180 per internal IP $1000 per external IP	$42,500	$11,000

Network Remediation Costs			
Ponemon Institute		Kaspersky Labs[219]	
2012 Report[220]	2015 Report[221]	Enterprise Networks	Small/Medium Businesses
$591,780	$973,130	$551,000	$38,000

The costs for the vulnerability scanner licenses, vulnerability assessments, penetration testing, and network remediation is likely to be on the upper end of the cost scale. Buying the scanner licenses in a block or in quantity may lower the cost per license. Also, DOD contracting agencies can likely achieve a lower price for all these cost items when negotiating with the individual service providers. Lastly, as discussed previously, these program elements are cost sharing measures. The DOD is not going to bear the full amount of these costs.

---

215 "MainNerve Penetration Testing," MainNerve.com, accessed March 30, 2016, http://mainnerve.calls.net/pentest/?pmc=G-pentest&gclid=COOv77yz5MsCFUlufgodMWIJGw.

216 Kim Christensen (V.P. Customer Development of Mainnerve.com), in phone call with author, April 5, 2016.

217 Darrell Boyd (Sales Officer at Convergence Technology), "Re: Vulnerability Assessment/Pen Testing," in email message to author, April 28, 2016.

218 Gregory Boudah (Sales Officer at Core Security), "RE: Core Security More info Request," In email message to author, March 28, 2016.

219 Kaspersky Lab, "Damage Control: The Cost of Security Breaches," 2 (2015).

220 Ponemon Institute, sponsored by Hewlett Packard, "2012 Cost of Cyber Crime Study: United States," 5 (2012).

221 Ponemon Institute, sponsored by Hewlett Packard, "2015 Cost of Cyber Crime Study: Global," 5 (2015).

E. SUMMARY

In this chapter, a significant restructuring and increase in scope for the current DOD DIB CS/IA Program is recommended. The successful implementation of these recommendations will require a significant investment in both emphasis and resources toward the enhanced program by both the DOD and DIB participants. The DOD must direct additional effort, manpower, and funding to the enhanced program to adequately incentivize it in order to influence DIB participants to achieve improved network security. The DIB participants must also invest additional resources in order to meet the enhanced program's network security requirements. However, if both parties are willing to fully commit to the enhanced program and make the necessary investments, then both parties will have an opportunity to reap significant benefits from the enhanced program. The DIB participants stand to gain improved network security with assistance from the DOD, significant financial incentives reduced liability risk, and reduced financial risk. The DODIN's security will improve because improved security of third-party networks that contact the DODIN will close off many potential attack vectors into the DODIN. So by assisting the DIB participants and providing stronger incentives to improve their network security, the DOD stands to gain improved security for the DODIN and, consequently, reduced operational risk.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

Completely securing information networks and driving the risk of network breaches to zero are impossible tasks. Software programing and network architectures have become so dynamic and complex that it is effectively impossible to know every detail of the software and network systems an organization uses. Thus, attempting to completely secure networks becomes cost prohibitive and would require such restrictive security measures that networks would become nearly unusable. Conversely, poorly secured networks do not adequately mitigate risks of network breaches. So the task for network administrators is to appropriately manage the risk to their networks. The risk equation presented in Chapter II manages this problem by balancing acceptable risk levels with the controls required to achieve these levels.

Unfortunately, there are several reasons why many organizations fail to properly assess and manage the risk to their information networks. First, companies do not understand the enormous scope and capability of the threats their networks face,[222] and so they do not prioritize network security.[223] Second, as discussed in Chapter II, the full scope of cyber attack costs are extremely difficult to assess accurately. Additionally, some of the direct costs incurred due to cyber attacks are often born by other parties than the actual attack victim.[224] Consequently, companies fail to fully appreciate the financial risk they face from cyber attacks,[225][226] and thus make poor cost/benefit decisions for network security investments.[227] Kaspersky Lab supports these contentions with data that indicates, even as recently as of 2015, that only approximately 50 percent of IT

[222] McAfee Labs with Intel Security, McAfee Labs Threats Report, 9–10 (August 2015).

[223] Burns and Price, eds., *Securing Cyberspace: A New Domain for National Security*, 130.

[224] Benjamin Dean, "Sorry Consumers, Companies have little Incentive to Invest in Better Cybersecurity," *Quartz*, March 05, 2015, http://qz.com/356274/cybersecurity-breaches-hurt-consumers-companies-not-so-much/.

[225] Kaspersky Lab, "Damage Control: The Cost of Security Breaches," 6 (2015).

[226] CSIS, "The Economic Impact of Cybercrime and Cyber Espionage," 3 (2013).

[227] Burns and Price, eds., *Securing Cyberspace: A New Domain for National Security*, 132.

professionals list defending against network breaches as one of their top three concerns.[228] So companies will prioritize other business related-functions ahead of network security.[229] Thus, poor organizational cyber security is often the result of a lack of a security-based mindset, proper education in network security, and the will to enforce security.

The DOD is knowledgeable and experienced in analyzing risk to and prioritization of network security for the DODIN. However, due to the DODIN's size and scope, one of its significant security weaknesses is the number of third-party networks that routinely connect to it. The DOD itself has estimated that there are over 10,000 networks for DOD contractors alone.[230] Since the majority of these third-party networks do not belong to the federal government, the DOD cannot exercise authority over them. So the DOD finds it extremely difficult to influence these third-party networks' security posture. The current DOD DIB CS/IA Program is DOD's attempt to positively affect this lack of awareness and influence through information sharing and limited technical assistance to covered defense contractors. Unfortunately, the current program does not take bold enough steps to make a pronounced effect on the security posture of the third-party networks that contact the DODIN. As discussed in Chapter III, the current program limits participants to only covered defense contractors; consequently, it does not even address a large number of other third-party networks that may contact the DODIN. The current program also offers no real incentive for participating companies to take any significant action to improve their network security. Security professionals have recognized and stressed the need for governments to provide incentives for the private sector to more fully invest in network security.[231] So incentives are where the DOD must take a bolder approach with regards to influencing third-party network security. To achieve the largest impact, the incentives should be primarily financial risk and

---

[228] Kaspersky Lab, "Damage Control: The Cost of Security Breaches," 6 (2015).

[229] Burns and Price, eds., *Securing Cyberspace: A New Domain for National Security*, 133.

[230] Department of Defense (DOD)-Defense Industrial Base (DIB) Cybersecurity (CS) Activities, *Federal Register* 80, no 191, 59583 (October 2, 2015).

[231] Burns and Price, eds., *Securing Cyberspace: A New Domain for National Security*, 130.

assistance-based. The answer to the lack of incentive in the current DOD DIB CS/IA Program is the proposed Enhanced DOD CS/IA Program.

The Enhanced DOD CS/IA Program, through its tiered structure of network security requirements and incentives, will engage a broader scope of third-party networks that contact the DODIN. As explained in Chapter IV, the program's network security requirements will be based on NIST recommended security best practices. These security requirements will give the DOD a method to influence and assess the risk these third-party networks present to the DODIN. The program's incentive elements will provide the DOD mechanisms to attract organizations to the program and influence over their network security posture. On a more strategic level, the enhanced program will also allow the DOD to assume a greater role in protecting the private sector's information networks.

Some security professionals have made the argument that the government must take greater responsibility to protect and secure private information networks.[232] Should the federal government decide to seriously consider this argument, then another course of action for the Enhanced DOD CS/IA Program potentially exists. In this course of action, the federal government would give control of the enhanced program to DHS. Several reasons exist for why this course of action makes sense and should be considered. First, one of DHS's core missions is to work with the private sector to secure information networks.[233] So this program would fit clearly inside DHS's mission set. Second, due to its mission set, DHS has the ability to expand the program's effects further because DHS can apply it to the whole of government, meaning any organization that interacts with any part of the federal government and not just the DOD. Lastly, since the enhanced program is modeled on the Safety Act Program, DHS already has resident knowledge and experience operating a program with similar structure and function.

Political, military, and private sector leaders must understand that private sector information network security is directly linked to national security.[234] Consequently, in

---

[232] Ibid., 130–131.

[233] "Our Mission," Department of Homeland Security, accessed April 8, 2016, https://www.dhs.gov/our-mission.

[234] Burns and Price, eds., *Securing Cyberspace: A New Domain for National Security*, 129.

order to protect national security, a shift in mindset on network security must occur. The mindset must be that security, as well as risk assessment and mitigation are integral to all networks that support operations. The government must take the lead in order to ensure this mindset shift occurs.[235][236] The Enhanced DOD CS/IA Program, whether it remains a DOD program or potentially shifts to DHS, is a step forward in the government's leadership role in network security.

B. RECOMMENDATIONS

1. The Enhanced DOD CS/IA Program

The author recommends the DOD implement the Enhanced DOD CS/IA Program as it is presented in this thesis. In order to fully implement the enhanced program, the author recommends the DOD take the following actions:

- Work with Congress to create and pass legislation that would legally create the program's liability protections for participants
- Modify the DFARS to create the APLs, ASLs, and new contract bid evaluation criteria to support the program
- Further explore pricing and appropriate fiscal methods to support cost sharing for network remediation, vulnerability assessments, penetration testing, and vulnerability scanner licenses
- Develop the enhanced program's self-assessment checklist or form using the NIST Special Publications listed in this thesis
- Conduct troop-to-task and budgetary analyses on the DOD DIB CS/IA Program Office based on the enhanced program's requirements to determine appropriate program office staffing and funding requirements

To aid the first action, the original language used for the Safety Act legislation has been included in Appendix C.

2. Program Control

[235] Ibid., 135.

[236] Henry Kenyon, "U.S. Still Lacks Some Basic Essentials for Cyber Defense," *Defense Systems*, January 28, 2011, https://defensesystems.com/articles/2011/01/28/cyber-defense-remains-incomplete.aspx?admgarea=DS.

The author recommends that the DOD and DHS begin discussions to determine which department should operate and control the enhanced program. Both the DOD and DHS have specific interests and missions, but the two departments must evaluate this question from a perspective of how the enhanced program can serve these specific interests while also better serving the greater national interest. Consequently, the author recommends placing program control under DHS because dealing with the security of private sector information networks is already a DHS core mission and the program will have greater ability to reduce risk to whole of government and private sector under DHS. Ultimately, the decision must be made by where DOD and DHS assess the enhanced program can best reduce risk to government networks and improve private sector network security.

C. SUGGESTIONS FOR FUTURE WORK

While this thesis provides an example self-assessment form, additional work should be done to further refine this form. Additionally, work should be done to develop separate forms for companies that may have differing security categories based on their size and business type. The author recommends this be done as soon as possible. The finalization of the self-assessment form will be critical to how well the enhanced program is able to improve and maintain the participants' network security posture. This future work should ensure the previously discussed critical best practices from the NIST Special Publications are included into the checklist, while not making it too complicated or onerous for participants to use. This checklist could also prove beneficial to other governmental or private sector organizations looking for a structured, yet relatively simple way to assess their networks.

This thesis investigated the enhanced program's costs, but only for a rough order of magnitude. However, before the enhanced program is implemented, a full cost benefit analysis must be completed for the program. This cost benefit analysis will allow the DOD or DHS to better plan for program costs, as well as justify these costs to senior leadership and Congress. The cost benefit analysis information will also support a more thorough risk analyses for the DODIN.

Program metrics are an important aspect of the enhanced program, and they were not developed in this thesis. Therefore, before the program is implemented, the author recommends that well defined metrics be developed to allow program managers to determine if the enhanced program is meeting its security objectives. Metrics may also tell program managers where the enhanced program should be modified or adjusted to better achieve its security objectives. Lastly, good metrics will aid program managers in defending the program and its budgetary requirements to their superiors and to political leadership. Examples of metrics that should be considered are number of program participants, rate of new program applicants, the number/rate of attacks conducted against the DODIN through third-party networks, and the number/rate of companies that compromise DOD information due to network breaches. Though, many other metrics could be created as well.

Lastly, personnel and budgetary requirements for the program office were discussed in this thesis but not in great detail. The author recommends that a detailed troop-to-task and budget analysis be conducted for the program office based on the enhanced program's requirements. These analyses will be critical in determining the personnel staffing and funding levels necessary for the program office to effectively operate the enhanced program.

APPENDIX A. CURRENT U.S. TRANSCOM CONTRACTOR DATA

Table 8. U.S. TRANSCOM Contract Data[237]

Company	Date Awarded	Contract Number	Amount ($)
American President Lines Ltd. Inc.	February 25, 2016	HTC711-12-D-W003	128,565,957
Maersk Line Ltd.	February 25, 2016	HTC711-12-D-W013	113,917,789
Matson Navigation Co. Inc.	February 25, 2016	HTC711-12-D-W014	47,647,499
Hapag-Lloyd USA LLC	February 25, 2016	HTC711-12-D-W011	46,037,679
American Roll-on Roll-Off Carrier LLC	February 25, 2016	HTC711-12-D-W004	33,470,691
Farrell Lines Inc.	February 25, 2016	HTC711-12-D-W008	32,180,437
Liberty Global Logistics LLC	February 25, 2016	HTC711-12-D-W012	27,894,240
Central Gulf Lines Inc.	February 25, 2016	HTC711-12-D-W005	12,247,421
TransAtlantic Lines	February 25, 2016	HTC711-12-D-W023	10,298,060
TOTE Maritime Puerto Rico LLC	February 25, 2016	HTC711-12-D-W017	10,074,363
American Airlines Inc.	February 24, 2016	HTC711-13-D-C010	125,922,873
Alaska Airlines Inc.	January 15,2016	HTC711-13-D-C001	Share of: 125,922,873
Atlas Air Inc.	January 15,2016	HTC711-13-D-C002	Share of: 125,922,873
Federal Express Corp.	January 15,2016	HTC711-13-D-C003	Share of: 125,922,873
Kalitta Air LLC	January 15,2016	HTC711-13-D-C004	Share of: 125,922,873
Miami Air International Inc.	January 15,2016	HTC711-13-D-C005	Share of: 125,922,873
National Air Cargo Group Inc.	January 15,2016	HTC711-13-D-C006	Share of: 125,922,873

[237] "United States Transportation Command (TRANSCOM) Defense Contracts Listing," Military Industrial Complex, accessed April 26, 2016, http://www.militaryindustrialcomplex.com/us-transportation-command-defense-contracts-listing.asp.

Company	**Date Awarded**	**Contract Number**	**Amount ($)**
Northern Air Cargo Inc.	January 15,2016	HTC711-13-D-C007	Share of: 125,922,873
Omi Air International Inc.	January 15,2016	HTC711-13-D-C008	Share of: 125,922,873
United Parcel Service Co.	January 15,2016	HTC711-13-D-C009	Share of: 125,922,873
Totem Ocean Trailer Express Inc.	January 6, 2016	HTC711-16-D-W003	30,438795
Sea Star Line LLC	January 6, 2016	HTC711-16-D-W020	20,148,725
Young Brothers LTC	January 6, 2016	HTC711-16-D-W029	18,494,963

This data represents only a partial set of current U.S. TRANSCOM contracts. This set contains only those contracts awarded since January 1, 2016.

APPENDIX B. EXAMPLE ENHANCED DOD CS/IA PROGRAM SELF-ASSESSMENT FORM

The security control items in this example form are adapted from NIST SP 800–53[238] and NIST SP 800–171.[239] The items taken from NIST SP 800–53 are to secure information networks judged to have a low impact Security Category (SC). SC's are judged by how the three security objectives of confidentiality, integrity, and availability impact a network.[240] The definition of a low impact system is "an information system in which all three of the security objectives are low."[241] The DOD may decide that the private sector third-party networks it wants to influence are either moderate or high impact networks. This decision would affect the security control items from NIST SP 800–53 that are included on the self-assessment form.

The security controls items included in this example form are broken down into the 17 security control families for low impact networks listed in the NIST SP 800–53.[242] Supplemental guidance on these security control items can also be found in the NIST SP 800–53.

<u>SECURITY CONTROL FAMILY: ACCESS CONTROL (AC)</u>

1. Develops, documents, and disseminates to: to [*Assignment: organization-defined personnel or roles*]:

> a. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

---

[238] National Institute of Standards and Technology, *Special Publication 800–53 revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*, F-1 – F-233.

[239] National Institute of Standards and Technology, *Special Publication 800–171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, 9–14 (June 2015), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf.

[240] National Institute of Standards and Technology, *Special Publication 800–53 revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*, 28.

[241] Ibid.

[242] Ibid., 9 and E-3.

b. Procedures to facilitate the implementation of the access control policy and associated access controls.

2. Reviews and updates the current access control policy and procedures. [*Assignment: organization-defined frequency*].

3. Limits information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

4. Limits information system access to the types of transactions and functions that authorized users are permitted to execute.

5. Separates the duties of individuals to reduce the risk of malevolent activity without collusion.

6 Employs the principle of least privilege, including for specific security functions and privileged accounts.

7. Uses non-privileged accounts or roles when accessing non-security functions.

8. Prevents non-privileged users from executing privileged functions and audit the execution of such functions.

9. Limits unsuccessful logon attempts.

10. Uses session lock with pattern-hiding displays to prevent access/viewing of data after a period of inactivity.

11. Terminates (automatically) a user session after a defined condition.

12. Monitors and controls remote access sessions.

13. Employs cryptographic mechanisms to protect the confidentiality of remote access sessions.

14. Routes remote access via managed access control points.

15. Authorizes remote execution of privileged commands and remote access to security-relevant information.

16. Authorize wireless access prior to allowing such connections.

17. Protects wireless access using authentication and encryption.

18. Controls connection of mobile devices.

19. Verifies and controls/limits connections to and use of external information systems.

20. Limits use of organizational portable storage devices on external information systems.

21. Controls information posted or processed on publicly accessible information systems.

SECURITY CONTROL FAMILY: AWARENESS AND TRAINING (AT)

1. Develops, documents, and disseminates to: to [*Assignment: organization-defined personnel or roles*]:

> a. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
>
> b. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

2. Reviews and updates the current security awareness and training policy and procedures. [*Assignment: organization-defined frequency*].

3. The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

> a. As part of initial training for new users.
>
> b. When required by information system changes.
>
> c. [*Assignment: organization-defined frequency*] thereafter.

4. The organization provides role-based security training to personnel with assigned security roles and responsibilities:

> a. Before authorizing access to the information system or performing assigned duties.
>
> b. When required by information system changes.
>
> c. [*Assignment: organization-defined frequency*] thereafter.

5. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

6. Retains individual training records for [*Assignment: organization-defined time period*].

7. Ensures that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.

8. Provide security awareness training on recognizing and reporting potential indicators of insider threat.

SECURITY CONTROL FAMILY: AUDIT AND ACCOUNTABILITY (AU)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

> a. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
>
> b. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

2. Reviews and updates the current audit and accountability policy and procedures. [*Assignment: organization-defined frequency*].

3. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*].

4. Reports findings to [*Assignment: organization-defined personnel or roles*].

5. Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

6. Alert in the event of an audit process failure.

7. Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.

8. Provide audit reduction and report generation to support on-demand analysis and reporting.

9. Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

10. Protect audit information and audit tools from unauthorized access, modification, and deletion.

11. Limit management of audit functionality to a subset of privileged users.

SECURITY CONTROL FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION (CA)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

> a. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
>
> b. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.

2. Reviews and updates the current security assessment and authorization policy and procedures [*Assignment: organization-defined frequency*].

3. Develops a security assessment plan that describes the scope of the assessment including:

> a. Security controls and control enhancements under assessment.
>
> b. Assessment procedures to be used to determine security control effectiveness.
>
> c. Assessment environment, assessment team, and assessment roles and responsibilities.

4. Assesses the security controls in the information system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

5. Produces a security assessment report that documents the results of the assessment.

6. Provides the results of the security control assessment to [*Assignment: organization-defined individuals or roles*].

7. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements.

8. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.

9. Reviews and updates Interconnection Security Agreements [*Assignment: organization-defined frequency*].

10. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

11. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

12. Assigns a senior-level executive or manager as the authorizing official for the information system.

13. Ensures that the authorizing official authorizes the information system for processing before commencing operations.

14. Updates the security authorization [*Assignment: organization-defined frequency*].

15. The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of [*Assignment: organization-defined metrics*] to be monitored.

b. Establishment of [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessments supporting such monitoring.

c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.

d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.

e. Correlation and analysis of security-related information generated by assessments and monitoring.

f. Response actions to address results of the analysis of security-related information.

g. Reporting the security status of organization and the information system to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*].

16. Authorizes internal connections of [*Assignment: organization-defined information system components or classes of components*] to the information system.

17. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

SECURITY CONTROL FAMILY: CONFIGURATION MANAGEMENT (CM)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

a. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

b. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

2. Reviews and updates the current configuration management policy and procedures [*Assignment: organization-defined frequency*].

3. The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

4. The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

5. Develops and documents an inventory of information system components that:

a. Accurately reflects the current information system.

b. Includes all components within the authorization boundary of the information system.

c. Is at the level of granularity deemed necessary for tracking and reporting.

6. Reviews and updates the information system component inventory [*Assignment: organization-defined frequency*].

7. Establishes and enforces security configuration settings for information technology products employed in organizational information systems.

8. Defines, documents, approves, and enforce physical and logical access restrictions associated with changes to the information system.

9. Employs the principle of least functionality by configuring the information system to provide only essential capabilities.

10. Restricts, disables, and prevents the use of nonessential programs, functions, ports, protocols, and services.

11. Applies deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

12. Controls and monitors user-installed software.

SECURITY CONTROL FAMILY: CONTINGENCY PLANNING (CP)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

> a. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
>
> b. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

2. Reviews and updates the current contingency planning policy and procedures [*Assignment: organization-defined frequency*].

3. The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

> a. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility.
>
> b. When required by information system changes.
>
> c. [*Assignment: organization-defined frequency*] thereafter.

4. Tests the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the effectiveness of the plan and the organizational readiness to execute the plan.

5. Reviews the contingency plan test results.

6. Initiates corrective actions, if needed.

SECURITY CONTROL FAMILY: IDENTIFICATION AND AUTHENTICATION (IA)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

> a. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
>
> b. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

2. Reviews and updates the current identification and authentication policy and procedures [*Assignment: organization-defined frequency*].

3. Identifies information system users and processes acting on behalf of users or devices.

4. Authenticates (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

5. Uses multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

6. Employs replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

7. Prevents reuse of identifiers for a defined period.

8. Disables identifiers after a defined period of inactivity.

9. Enforces a minimum password complexity and change of characters when new passwords are created.

10. Prohibits password reuse for a specified number of generations.

11. Allows temporary password use for system logons with an immediate change to a permanent password.

12. Stores and transmits only encrypted representation of passwords.

13. Obscures feedback of authentication information.

SECURITY CONTROL FAMILY: INCIDENT RESPONSE (IR)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

> a. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
>
> b. Procedures to facilitate the implementation of the incident response policy and associated incident response controls.

2. Reviews and updates the current incident response policy and procedures [*Assignment: organization-defined frequency]*.

3. The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

> a. Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility.
>
> b. When required by information system changes.
>
> c. [*Assignment: organization-defined frequency*] thereafter.

4. Tracks, documents, and reports incidents to appropriate officials and/or authorities both internal and external to the organization.

5. Establishes an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

6. Tests the organizational incident response capability.

SECURITY CONTROL FAMILY: MAINTENANCE (MA)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

a. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

b. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.

2. Reviews and updates the current system maintenance policy and procedures [*Assignment: organization-defined frequency*].

3. Performs maintenance on organizational information systems.

4. Provides effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

5. Ensures equipment removed for off-site maintenance is sanitized.

6. Checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

7. Requires multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

8. Supervises the maintenance activities of maintenance personnel without required access authorization.

SECURITY CONTROL FAMILY: MEDIA PROTECTION (MP)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

a. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

b. Procedures to facilitate the implementation of the media protection policy and associated media protection controls.

2. Reviews and updates the current media protection policy and procedures [*Assignment: organization-defined frequency*].

3. Sanitize or destroy information system media before disposal or release for reuse.

4. Control the use of removable media on information system components.

5. Prohibit the use of portable storage devices when such devices have no identifiable owner.

SECURITY CONTROL FAMILY: PHYSICAL AND ENVIRONMENTAL (PE)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

> a. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
>
> b. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

2. Reviews and updates the current physical and environmental protection policy and procedures [*Assignment: organization-defined frequency*].

3. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents.

4. Limits physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

5. Reviews physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*].

6. Coordinates results of reviews and investigations with the organizational incident response capability.

7. Maintains visitor access records to the facility where the information system resides for [*Assignment: organization-defined time period*].

8. Escorts visitors and monitor visitor activity.

9. Reviews visitor access records [*Assignment: organization-defined frequency*].

SECURITY CONTROL FAMILY: PLANNING (PL)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

a. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

b. Procedures to facilitate the implementation of the security planning policy and associated security planning controls.

2. Reviews and updates the current security planning policy and procedures [*Assignment: organization-defined frequency*].

3. Develops a security plan for the information system that:

a. Is consistent with the organization's enterprise architecture.

b. Explicitly defines the authorization boundary for the system.

c. Describes the operational context of the information system in terms of missions and business processes.

d. Provides the security categorization of the information system including supporting rationale.

e. Describes the operational environment for the information system and relationships with or connections to other information systems.

f. Provides an overview of the security requirements for the system.

g. Identifies any relevant overlays, if applicable.

h. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions.

i. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

4. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*].

5. Reviews the security plan for the information system [*Assignment: organization-defined frequency*].

6. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

7. Protects the security plan from unauthorized disclosure and modification.

8. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.

9. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

10. Reviews and updates the rules of behavior [*Assignment: organization-defined frequency*].

11. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

SECURITY CONTROL FAMILY: PERSONNEL SECURITY (PS)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

> a. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
>
> b. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

2. Reviews and updates the current personnel security policy and procedures [*Assignment: organization-defined frequency*].

3. Develops and documents access agreements for organizational information systems.

4. Reviews and updates the access agreements [*Assignment: organization-defined frequency*].

5. Ensures that individuals requiring access to organizational information and information systems:

> a. Sign appropriate access agreements prior to being granted access.
>
> b. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [*Assignment: organization-defined frequency*].

6. Establishes personnel security requirements including security roles and responsibilities for third-party providers.

7. Requires third-party providers to comply with personnel security policies and procedures established by the organization.

8. Documents personnel security requirements.

9. Requires third-party providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*Assignment: organization-defined time period*].

10. Monitors provider compliance.

11. Screens individuals prior to authorizing access to information systems containing CUI.

12. Ensures information systems are protected during and after personnel actions such as terminations and transfers.

<u>SECURITY CONTROL FAMILY: RISK ASSESSMENT (RA)</u>

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

> a. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
>
> b. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

2. Reviews and updates the current risk assessment policy and procedures [*Assignment: organization-defined frequency*].

3. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

4. Documents risk assessment results in [*Selection: security plan; risk assessment report*; [*Assignment: organization-defined document*]].

5. Reviews risk assessment results [*Assignment: organization-defined frequency*].

6. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*].

7. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

8. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined proces*s] and when new vulnerabilities potentially affecting the system/applications are identified and reported.

9. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for.

a. Enumerating platforms, software flaws, and improper configurations.

b. Formatting checklists and test procedures.

c. Measuring vulnerability impact.

10. Analyzes vulnerability scan reports and results from security control assessments.

11. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk.

12. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

SECURITY CONTROL FAMILY: SYSTEM AND SERVICES ACQUISITION (SA)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

a. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

b. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

2. Reviews and updates the current system and services acquisition policy and procedures [*Assignment: organization-defined frequency*].

3. Determines information security requirements for the information system or information system service in mission/business process planning.

4. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process.

5. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

6. Manages the information system using [*Assignment: organization-defined system development life cycle*] that incorporates information security considerations.

7. Defines and documents information security roles and responsibilities throughout the system development life cycle.

8. Identifies individuals having information security roles and responsibilities.

9. Integrates the organizational information security risk management process into system development life cycle activities.

10. The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements.

b. Security strength requirements.

c. Security assurance requirements.

d. Security-related documentation requirements.

e. Requirements for protecting security-related documentation.

f. Description of the information system development environment and environment in which the system is intended to operate.

g. Acceptance criteria.

11. The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

12. Obtains administrator documentation for the information system, system component, or information system service that describes:

a. Secure configuration, installation, and operation of the system, component, or service.

b. Effective use and maintenance of security functions/mechanisms.

c. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

13. Obtains user documentation for the information system, system component, or information system service that describes:

a. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.

b. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner.

c. User responsibilities in maintaining the security of the system, component, or service.

14. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes [*Assignment: organization-defined actions*] in response.

15. Protects documentation as required, in accordance with the risk management strategy.

16. Distributes documentation to [*Assignment: organization-defined personnel or roles*].

17. Requires that providers of external information system services comply with organizational information security requirements and employ [*Assignment: organization-defined security controls*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

18. Defines and documents government oversight and user roles and responsibilities with regard to external information system services.

19. Employs [*Assignment: organization-defined processes, methods, and techniques*] to monitor security control compliance by external service providers on an ongoing basis.

SECURITY CONTROL FAMILY: SYSTEM AND COMMUNICATION PROTECTION (SC)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

a. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

b. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

2. Reviews and updates the current system and communications protection policy and procedures [*Assignment: organization-defined frequency*].

3. The information system maintains a separate execution domain for each executing process.

4. Monitors, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

5. Employs architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

6. Separates user functionality from information system management functionality.

7. Prevents unauthorized and unintended information transfer via shared system resources.

8. Implements subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

9. Denys network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

10. Prevents remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.

11. Terminates network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

12. Establishes and manage cryptographic keys for cryptography employed in the information system.

13. Prohibits remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

14. Controls and monitor the use of mobile code.

15. Controls and monitor the use of Voice over Internet Protocol (VoIP) technologies.

16. Protects the authenticity of communications sessions.

SECURITY CONTROL FAMILY: SYSTEM AND INFORMATION INTEGRITY (SI)

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

> a. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
>
> b. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

2. Reviews and updates the current system and information integrity policy and procedures [*Assignment: organization-defined frequency*].

3. Monitors the information system to detect:

> a. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*].
>
> b. Unauthorized local, network, and remote connections.
>
> c. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*].

4. Deploys monitoring devices:

> a. Strategically within the information system to collect organization-determined essential information.
>
> b. At ad hoc locations within the system to track specific types of transactions of interest to the organization.

5. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

6. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

7. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

8. Provides [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed*; [*Assignment: organization-defined frequency*]].

9. Receives information system security alerts, advisories, and directives from [*Assignment: organization-defined external organizations*] on an ongoing basis.

10. Generates internal security alerts, advisories, and directives as deemed necessary.

11. Disseminates security alerts, advisories, and directives to: [*Selection (one or more)*: [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined elements within the organization*]; [*Assignment: organization-defined external organizations*]].

12. Provides protection from malicious code at appropriate locations within organizational information systems.

13. Updates malicious code protection mechanisms when new releases are available.

14. Performs periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

15. Monitors the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

16. Identifies unauthorized use of the information system.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. SAFETY ACT LEGISLATION TEXT

The following text is Subtitle G—Support Anti-terrorism by Fostering Effective Technologies Act of 2002, of Title VIII of the Homeland Security Act of 2002.[243] The text was copied directly from the Homeland Security Act of 2002. It is meant to provide example language for legislation that would support the liability protections contained in the Enhanced DOD CS/IA Program. The legislation's text can also be found on DHS Safety Act website at: https://www.safetyact.gov/jsp/refdoc/samsRefDocSearch.do.[244]

[243] Homeland Security Act of 2002, Pub. L. No. 107–296, 116 Stat. 2135 (November 25, 2002).

[244] "Safety Act: Printer Friendly Materials," Department of Homeland Security, accessed May 31, 2016, https://www.safetyact.gov/jsp/refdoc/samsRefDocSearch.do.

Subtitle G—Support Anti-terrorism by Fostering Effective Technologies Act of 2002

SEC. 861. SHORT TITLE.
This subtitle may be cited as the ''Support Anti-terrorism by Fostering Effective Technologies Act of 2002'' or the ''SAFETY Act''.

SEC. 862. ADMINISTRATION.
(a) IN GENERAL.—The Secretary shall be responsible for the administration of this subtitle.

(b) DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES.
—The Secretary may designate anti-terrorism technologies that qualify for protection under the system of risk management set forth in this subtitle in accordance with criteria that shall include, but not be limited to, the following:

(1) Prior United States Government use or demonstrated substantial utility and effectiveness.

(2) Availability of the technology for immediate deployment in public and private settings.

(3) Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of such anti-terrorism technology.

(4) Substantial likelihood that such anti-terrorism technology will not be deployed unless protections under the system of risk management provided under this subtitle are extended.

(5) Magnitude of risk exposure to the public if such antiterrorism technology is not deployed.

(6) Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm.

(7) Anti-terrorism technology that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat or respond to such acts.

(c) REGULATIONS.—The Secretary may issue such regulations, after notice and comment in accordance with section 553 of title 5, United States Code, as may be necessary to carry out this subtitle.

SEC. 863. LITIGATION MANAGEMENT.
(a) FEDERAL CAUSE OF ACTION.—
(1) IN GENERAL.—There shall exist a Federal cause of action for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. The substantive law for decision in any such action shall be derived from the law, including choice of law principles, of the State in which such acts of terrorism occurred, unless such law is inconsistent with or preempted by Federal law. Such Federal cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism technology to Federal and non-Federal government customers.

(2) JURISDICTION.—Such appropriate district court of the United States shall have original and exclusive jurisdiction over all actions for any claim for loss of property, personal injury, or death arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller.

(1) PUNITIVE DAMAGES.—No punitive damages intended to punish or deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses may be awarded, nor shall any party be liable for interest prior to the judgment.

(2) NONECONOMIC DAMAGES.—

(A) IN GENERAL.—Noneconomic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff, and no plaintiff may recover noneconomic damages unless the plaintiff suffered physical harm.

(B) DEFINITION.—For purposes of subparagraph (A), the term ''noneconomic damages'' means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship,
loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.

(c) COLLATERAL SOURCES.—Any recovery by a plaintiff in an action under this section shall be reduced by the amount of collateral source compensation, if any, that the plaintiff has received or is entitled to receive as a result of such acts of terrorism that result or may result in loss to the Seller.

(d) GOVERNMENT CONTRACTOR DEFENSE.—
(1) IN GENERAL.—Should a product liability or other lawsuit be filed for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies approved by the Secretary, as provided in paragraphs (2) and (3) of this subsection, have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller, there shall be a rebuttable presumption that the government contractor defense applies in such lawsuit. This presumption shall only be overcome by evidence showing that the Seller acted fraudulently or with
willful misconduct in submitting information to the Secretary during the course of the Secretary's consideration of such technology under this subsection. This presumption of the government contractor defense shall apply regardless of whether the claim against the Seller arises from a sale of the product to Federal Government or non-Federal Government customers.

(2) EXCLUSIVE RESPONSIBILITY.—The Secretary will be exclusively responsible for the review and approval of antiterrorism technology for purposes of establishing a government contractor defense in any product liability lawsuit for claims arising out of, relating to, or resulting from an act of terrorism
when qualified anti-terrorism technologies approved by the Secretary, as provided in this paragraph and paragraph (3), have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. Upon the Seller's submission to the Secretary for approval of anti-terrorism technology, the Secretary will conduct a comprehensive review of the design of such technology and determine whether it will perform as intended, conforms to the Seller's specifications, and is safe for use as intended. The Seller will conduct safety and hazard analyses on such technology and will supply the Secretary with all such information.

(3) CERTIFICATE.—For anti-terrorism technology reviewed and approved by the Secretary, the Secretary will issue a certificate of conformance to the Seller and place the antiterrorism technology on an Approved Product List for Homeland Security.
(e) EXCLUSION.—Nothing in this section shall in any way limit the ability of any person to seek any form of recovery from any person, government, or other entity that—
(1) attempts to commit, knowingly participates in, aids and abets, or commits any act of terrorism, or any criminal act related to or resulting from such act of terrorism; or (2) participates in a conspiracy to commit any such act of terrorism or any such criminal act.

SEC. 864. RISK MANAGEMENT.

(a) IN GENERAL.—

(1) LIABILITY INSURANCE REQUIRED.—Any person or entity that sells or otherwise provides a qualified anti-terrorism technology to Federal and non-Federal Government customers (''Seller'') shall obtain liability insurance of such types and in such amounts as shall be required in accordance with this section and certified by the Secretary to satisfy otherwise compensable third-party claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act.

(2) MAXIMUM AMOUNT.—For the total claims related to 1 such act of terrorism, the Seller is not required to obtain liability insurance of more than the maximum amount of liability insurance reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price of Seller's anti-terrorism technologies.

(3) SCOPE OF COVERAGE.—Liability insurance obtained pursuant to this subsection shall, in addition to the Seller, protect the following, to the extent of their potential liability for involvement in the manufacture, qualification, sale, use, or operation of qualified anti-terrorism technologies deployed in defense against or response or recovery from an act of terrorism:

(A) Contractors, subcontractors, suppliers, vendors and customers of the Seller.

(B) Contractors, subcontractors, suppliers, and vendors of the customer.

(4) THIRD PARTY CLAIMS.—Such liability insurance under this section shall provide coverage against third party claims arising out of, relating to, or resulting from the sale or use of anti-terrorism technologies.

(b) RECIPROCAL WAIVER OF CLAIMS.—The Seller shall enter into a reciprocal waiver of claims with its contractors, subcontractors, suppliers, vendors and customers, and contractors and subcontractors of the customers, involved in the manufacture, sale, use or operation of qualified anti-terrorism technologies, under which each party to the waiver agrees to be responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act.

(c) EXTENT OF LIABILITY.—Notwithstanding any other provision of law, liability for all claims against a Seller arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller, whether for compensatory or punitive damages or for contribution or indemnity, shall not be in an amount greater than the limits of liability insurance coverage required to be maintained by the Seller under this section.

SEC. 865. DEFINITIONS.

For purposes of this subtitle, the following definitions apply:

(1) QUALIFIED ANTI-TERRORISM TECHNOLOGY.—For purposes of this subtitle, the term ''qualified anti-terrorism technology'' means any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary.

(2) ACT OF TERRORISM.—(A) The term ''act of terrorism'' means any act that the Secretary determines meets the requirements under subparagraph (B), as such requirements are further defined and specified by the Secretary.

(B) REQUIREMENTS.—An act meets the requirements of this subparagraph if the act—

(i) is unlawful;

(ii) causes harm to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States; and (iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.

(3) INSURANCE CARRIER.—The term ''insurance carrier'' means any corporation, association, society, order, firm, company, mutual, partnership, individual aggregation of individuals, or any other legal entity that provides commercial property and casualty insurance. Such term includes any affiliates of a commercial insurance carrier.

(4) LIABILITY INSURANCE.—
(A) IN GENERAL.—The term ''liability insurance'' means insurance for legal liabilities incurred by the insured resulting from—

(i) loss of or damage to property of others;
(ii) ensuing loss of income or extra expense incurred because of loss of or damage to property of others;
(iii) bodily injury (including) to persons other than the insured or its employees; or
(iv) loss resulting from debt or default of another.
(5) LOSS.—The term ''loss'' means death, bodily injury, or loss of or damage to property, including business interruption loss.

(6) NON-FEDERAL GOVERNMENT CUSTOMERS.—The term ''non-Federal Government customers'' means any customer of a Seller that is not an agency or instrumentality of the United States Government with authority under Public Law 85–804 to provide for indemnification under certain circumstances for third-party claims against its contractors, including but not limited to State and local authorities and commercial entities.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Acunetix Blog, The. http://www.acunetix.com/blog/news/anonymous-hack-us-department-of-defence-analysis/.

Assistant Secretary of Defense (NII). *Defense Industrial Base (DIB) Cyber Security/ Information Assurance (CS/IA) Activities*. DOD Instruction 5205.13. Washington, DC: Assistant Secretary of Defense (NII), January 29, 2010. http://www.dtic.mil/ whs/directives/corres/pdf/520513p.pdf.

Bernik, Igor. "Cybercrime: The Cost of Investments Into Protection." *Journal of Criminal Justice and Security* 16, no. 2 (2014): 105–116.

BeyondTrust. "Retina Network Security Scanner." Accessed March 29, 2016. http://shop.beyondtrust.com/ store?SiteID=eeyeinc&Action=DisplayProductDetailsPage&productID=285899100&pgm=94163000.

Blanchard, Benjamin S. *System Engineering Management*, 4th ed. Hoboken, NJ: John Wiley & Sons, 2008.

Burns, Nicholas and Jonathon Price, eds. *Securing Cyberspace: A New Domain for National Security*. Queenstown, MD: Aspen Institute, February 2012.

Center for Internet Security. *The CIS Critical Security Controls for Effective Cyber Defense Version 6.0*. (October 15, 2015). https://www.cisecurity.org/critical-controls.cfm.

Center for Strategic and International Studies. "The Economic Impact of Cybercrime and Cyber Espionage." (2013). http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4.pdf.

Chairman of the Joint Chiefs of Staff (CJCS). *Joint Capabilities Integration and Development System (JCIDS)*. CJCS Instruction 3170.01I. Washington, DC: Chairman of the Joint Chiefs of Staff (CJCS), January 23, 2015. http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01a.pdf.

Clark, Michael and Charles Harrell, "Unlike Chess Everyone Must Continue Playing after a Cyber Attack," *Journal of Investment Compliance* 14, no. 2 (2013): 5–12. DOI 10.1108/JOIC-10-2013-0034.

Clinton, Larry. "The Value Proposition for Cyber Security: Does it Exist and How can We Create it." Internet Security Alliance (2006). http://www.isalliance.org/ presentation/1_ISA_Overview_Presentations/ 2006_12_00_Larry_Clinton_Commerce_Department_Presentation.pdf.

Crosman, Penny. "Target Breach was Months in the Making." *American Banker*, February 12, 2014. http://search.proquest.com/docview/1497400210?accountid=12702.

Dean, Benjamin. "Sorry Consumers, Companies Have Little Incentive to Invest in Better Cybersecurity." *Quartz*. March 05, 2015. http://qz.com/356274/cybersecurity-breaches-hurt-consumers-companies-not-so-much/.

Department of Defense. *Defense Acquisition Guidebook*. (2013). https://acc.dau.mil/docs/dag_pdf/dag_complete.pdf.

Department of Defense. *DIB Cybersecurity Activities Fact Sheet: DOD—DIB Cybersecurity Information Sharing Program Overview*. (October 6, 2015). http://dodcio.defense.gov/.

Department of Defense. "(DOD)-Defense Industrial Base (DIB) Cybersecurity (CS) Activities." *Federal Register* 80, no. 191. (October 2, 2015): 59581-59583.

Department of Defense. "(DOD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities." *Federal Register* 77, no. 92 (May 11, 2012): 27615-27617

Department of Defense. *DOD's DIB CS/IA Program: A Public-Private Cyber Security Partnership*. 1–10 (April 22, 2014). http://www.dtic.mil/ndia/2014cyber/Michetti.pdf.

Department of Defense. Defense Federal Acquisition Regulations Supplement, Clause 252.204-7012. *Safeguarding of Unclassified Controlled Technical Information*. (November 2013). http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm.

Department of Defense, Defense Science Board Task Force on Resilient Military Systems. *Resilient Military Systems and the Advanced Cyber Threat*. (2013). http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

Department of Defense, Defense Security Service. *2015 Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting*. (2015). http://www.dss.mil/ci/ci_reports.html.

Department of Homeland Security. "Our Mission." Accessed April 8, 2016. https://www.dhs.gov/our-mission.

Department of Homeland Security, Science and Technology Directorate. "Safety Act: Printer Friendly Materials." Accessed May 31, 2016. https://www.safetyact.gov/jsp/refdoc/samsRefDocSearch.do.

Department of Homeland Security, Science and Technology Directorate. *SAFETY Act Fact Sheet*. (January 14, 2016). https://www.safetyact.gov/pages/homepages/Home.do.

Department of Homeland Security, Science and Technology Directorate, Office of SAFETY Act Implementation. *SAFETY Act 101Briefing: The Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002*. 1–27. https://www.safetyact.gov/pages/homepages/Home.do.

Department of Homeland Security, Science and Technology Directorate, Office of SAFETY Act Implementation. *SAFETY Act Webinar: The SAFETY Act and Business: Protecting You and Informing Your Customers*. 1–22 (December 02, 2015). https://www.safetyact.gov/jsp/refdoc/samsRefDocSearch.do.

Department of Homeland Security, Science and Technology Directorate, Office of SAFETY Act Implementation. *SAFETY Act Webinar: What is the SAFETY Act and How do You Apply*? 1–24 (February 11, 2015). https://www.safetyact.gov/jsp/refdoc/samsRefDocSearch.do.

Dinh. Thang N., Ying Xuan, My T. Thai, M, Panos M. Pardalos, and Taieb Znati. (2012). On New Approaches of Assessing Network Vulnerability: Hardness and Approximation. *IEEE/ACM Transactions on Networking*, 20, 609–619. doi: 10.1109/TNET.2011.2170849.

DOJ official: Companies can Make it Harder for Hackers to Succeed. (2015). *Inside Cybersecurity*, Retrieved from http://search.proquest.com/docview/1685156440?accountid=12702.

Dwivedi, Anurag and Dan Tebben. (2012). Cyber Situational Awareness and Differential Hardening. *SPIE Proceedings*, 8408, 1–8. doi: 10.1117/12.915642.

Finkle, Victoria. "Lawmakers Unveil Data Security Bill, Citing Target Breach." *American Banker*, January 16, 2014. http://search.proquest.com/docview/1490680935?accountid=12702.

Fulp, John D., "Network Security Core Principles." (lecture slides, Naval Postgraduate School, Monterey, CA February 2016).

Gandel, Stephen. "Lloyd's CEO: Cyber Attacks Cost Companies $400 Billion Every Year." *Fortune*, January 23, 2015. http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/.

Goldstein, Daniel, J. "Amid Cyber Threat to Your Business Data, Trust but Verify Third-Party Processing." *Mortgage Banking*, July 2015, 75(10), 85–86.

Gorman, Siobhan, August Cole, and Yochi Dreazen. "Computer Spies Breach Fighter-Jet Project." *The Wall Street Journal*, April 21, 2009. http://www.wsj.com/articles/SB124027491029837401.

GovTrack.us. "S. 961: Data Security Act of 2015." Accessed December 2, 2015. https://www.govtrack.us/congress/bills/114/s961.

Hackett, Robert. "How Much do Data Breaches Actually Cost Big Companies." *Fortune*, April 1, 2015. http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/.

Hemanidhi, Aniwat, Sanon Chimmanee, and Parinya Sanguansat. "Network Risk Evaluation from Security Metric of Vulnerability Detection Tools," *2014 IEEE Region 10 Conference*, (2014): 1–6, doi: 10.1109/TENCON.2014.7022358.

Homeland Security Act of 2002. Pub. L. No. 107–296. 116 Stat. 2135 (November 25, 2002).

Hughes, Jeff, and George Cybenko. (2014). Three Tenets for Secure Cyber-Physical System Design and Assessment. *SPIE Proceedings*, 9097, 1–15. doi: 10.1117/12.2053933.

Kaspersky Lab. "Damage Control: The Cost of Security Breaches." (2015). http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf.

Keller, John. "Defense Industry Concerned about Cyber Security; not sure Where to Turn for Help." *Military & Aerospace Electronics* 21, no. 6 (June 2015): 5–9.

Kenyon, Henry. "U.S. Still Lacks Some Basic Essentials for Cyber Defense." *Defense Systems*, January 28, 2011. https://defensesystems.com/articles/2011/01/28/cyber-defense-remains-incomplete.aspx?admgarea=DS.

Kerner, Sean M. "Home Depot Breach Expands, Privilege Escalation Flaw to Blame," *EWeek*, November 8, 2014, http://www.eweek.com/security/home-depot-breach-expands-privilege-escalation-flaw-to-blame.html.

Kroll, Karen. "Are Your Business Partners Letting in the Hackers?" *Compliance Week*. November 25, 2014. 64–72. http://web.b.ebscohost.com.libproxy.nps.edu.

Lynn III, William J, "Defending a New Domain." *Foreign Affairs*, September/October 2010, 97–108.

MainNerve. "MainNerve Penetration Testing." accessed March 30, 2016. http://mainnerve.calls.net/pentest/?pmc=G-pentest&gclid=COOv77yz5MsCFUlufgodMWIJGw.

McAfee Labs. *McAfee Labs Threat Report*. (May, 2015). http://www.mcafee.com/us/mcafee-labs.aspx.

McAfee Labs. *McAfee Labs Threat Report*. (August, 2015). http://www.mcafee.com/us/mcafee-labs.aspx.

McClure, Stuart, Joel Scambray, and George Kurtz. *Hacking Exposed*, 7th ed. New York, NY: McGraw-Hill, 2012.

Military Industrial Complex. "United States Transportation Command (TRANSCOM) Defense Contracts Listing." Accessed April 26, 2016. http://www.militaryindustrialcomplex.com/us-transportation-command-defense-contracts-listing.asp.

Mills, Elinor. "Pentagon Spends over $100 Million on Cyberattack Cleanup." *CNET News*. April 7, 2009. http://news.cnet.com/8301-1009_3-10214416-83.html.

Mitchell, Charlie. "Carper: Bill in the Works to Speed Deployment of Cyber Tool." *Inside Cybersecurity*. June 25, 2015. https://insidecybersecurity.com/daily-news/carper-bill-works-speed-deployment-cyber-tool.

New York State Department of Financial Services. (2015, April). *Update on Cyber Security in the Banking Sector: Third-party Service Providers*. Retrieved from http://www.dfs.ny.gov/.

Nichols, Robert, Susan Booth Cassidy, Anuj Vohra, Kayleigh Scalzo, and Catlin Meade. "Cyber Security for Government Contractors." *Briefing Papers* 14 no.5 (April 2014): 1–28. https://www.cov.com/files/Publication/42df1e52-f857-4459-8e3b-41383ca6919f/Presentation/PublicationAttachment/313eea21-adca-4e00-8eac-561a6f0d15a6/Cybersecurity_for_Govt_Contractors.pdf.

National Institute of Standards and Technology. *Special Publication 800–53 revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*. (April 2013). http://dx.doi.org/10.6028/NIST.SP.800-53r4.

National Institute of Standards and Technology. *Special Publication 800–115: Technical Guide to Information Security Testing and Assessment*. 6–1 (September 2008). http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

National Institute of Standards and Technology. *Special Publication 800–171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. (June 2015), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf.

Nunnally, Troy, A. S. Uluagac, John A. Copeland, and Raheem Beyah. (2012). 3DSVAT: A 3D Stereoscopic Vulnerability Assessment Tool for Network Security. *37th Annual IEEE Conf. on Local Computer Networks*. Clearwater, FL. doi: 10.1109/LCN.2012.6423586.

Office of Management and Budget. *Improving Cybersecurity Protections in Federal Acquisitions*. (n.d.). https://policy.cio.gov/.

Office of Personnel Management. *2016 General Schedule (Base) Salary Table (Annual Rate)*. 2016. https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2016/general-schedule/.

Paganini, Pierluigi. Another Computer System at the Pentagon Has Been Hacked. *Security Affairs*. September 11, 2015. http://securityaffairs.co/wordpress/40039/cyber-crime/pentagon-hacked-again.html.

Pandey, Sadhir K., Vivek K. Yadav, Sandeep Kumar, Shani Verma, and Prabhat Dansena. "Implementation of A New Framework for Automated Network Security Checking and Alert System" *2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN)*, (2014): 1–7, doi: 10.1109/WOCN.2014.6923089.

PCI Security Standards Council. "Information Supplement: Third-Party Security Assurance." (August 2014). https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf.

Ponemon Institute, sponsored by Hewlett Packard. "2015 Cost of Cyber Crime Study: Global." (2015). http://www.ponemon.org/library/2015-cost-of-cyber-crime-united-states.

Ponemon Institute, sponsored by Hewlett Packard. "2015 Cost of Cyber Crime Study: United States." (2015). http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

Presidential Executive Order 13636—Improving Critical Infrastructure Cybersecurity. *Federal Register*, 78(33), 11739-11744 (February 13, 2013). http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

Regulations implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act). *Federal Register* 71, no. 110. 33148 (June 8, 2006).

Saadawi, Tarek and Louis Jordan, eds. *Cyber Infrastructure Protection*. (2011).http://www.StrategicStudiesInstitute.army.mil/.

Sabovich, Jason R. and James A. Borst. "Remediating Third-Party Software Vulnerabilities on U.S. Army Information Systems." Master's thesis, Naval Postgraduate School, 2012. http://hdl.handle.net/10945/7410.

Scully, Tim. "The Cyber Security Threat Stops in the Boardroom." *Journal of Business Continuity & Emergency Planning* 7, no. 2 (Winter 2013/2014): 138–148.

Senate Committee on Armed Services. *Inquiry in Cyber Intrusions Affecting U.S. Transportation Command Contractors*. 113th Cong. (September 17, 2014).

Senate Committee on Commerce, Science, and Transportation. *A "Kill Chain" Analysis of the 2013 Target Data Breach*. U.S. Senate, 113th Cong. (2014).

Single Mobility System 10.3.0. "SMS." Accessed April 16, 2016, https://sms.transcom.mil/sms-perl/smswebstart.pl.

Smith, G. Steven, and Anthony J. Amoruso. "Using Real Options to Value Losses from Cyber Attacks." *Journal of Digital Asset Management* 2, no. 3/4 (May 2006): 150–162.

Tehan, R. (2015, January 9). *Cybersecurity: Authoritative Reports and Resources, by Topic*. Retrieved from the Congressional Research Service reports website: https://www.fas.org/sgp/crs/misc/index.html.

Tenable Network Security. "Nessus Professional." Accessed April 28, 2016. https://store.tenable.com/?main_page=index&cPath=23.

"UL, Cited as Model for Cyber Testing, has own Initiative Underway." *Inside Cybersecurity*, July 7, 2015. http://search.proquest.com/docview/1694696588?accountid=12702.

Under Secretary of Defense (AT&L). *The Defense Acquisition System*. DOD Directive 5000.1. Washington, DC: Under Secretary of Defense (AT&L), November 20, 2007. http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf.

United States Computer Emergency Readiness Team. *C3 Voluntary Program, C³ Voluntary Program Outreach and Messaging Kit: Cyber Risk Management Primer for CEOs*. (n.d.). https://www.us-cert.gov/ccubedvp.

United States Congress. *National Defense Authorization Act for Fiscal Year 2013*. 112th Congress. (2012) http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf.

Verizon Enterprise. "2014 Data Breach Investigations Report." (2014). http://www.verizonenterprise.com/DBIR/2014/?utm_source=earlyaccess&utm_medium=redirect&utm_campaign=DBIR.

Widmer, Lori. “10 Costliest Data Breaches.” *National Underwriter/Life & Health Financial Services* 119, no. 7 (July 2015): 45–46.

“White House Science Office Spurs Effort to Create Cyber Certification Lab.” *Inside Cybersecurity*, June 30, 2015. http://search.proquest.com/docview/1692270352?accountid=12702.

“Working with Third-Parties: Make Security a Priority.” *SC Magazine: For IT Security Professionals (UK Edition)*, July-August 2014. 8. http://www.scmagazineuk.com/working-with-third-parties-make-security-a-priority/article/357460/.

Yoon, Jun, and Wontae Sim. “Implementation of the Automated Network Vulnerability Assessment Framework,” *4th International Conference on Information Technology, 2007*, (2007): 153–157, doi: 10.1109/IIT.2007.4430423.

Yu, Wei, Sixiao Wei., Dan Shen,Misty Blowers, Erik P. Blasch, Khanh D. Pham, Genshe Chen, Hanlin Zhang, and Chao Lu. (2013). On Detection and Visualization Techniques for Cyber Security Situation Awareness. *SPIE Proceedings*, 8739, 1–9. doi: 10.1117/12.2015887.

Zeller, Randel L. *Bridging Technology Capability Gaps: Opportunities with the Private Sector*. Department of Homeland Security, Science and Technology Directorate, Interagency Office. 1–42. http://www.dtic.mil/ndia/2011jointmissions/TuesdayZeller.pdf.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California