NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

REGIONAL SECURITY ASSESSMENTS: A STRATEGIC APPROACH TO SECURING FEDERAL FACILITIES

by

Todd Consolini

December 2009

Thesis Advisor:	John Rollins
Second Reader:	Rudy Darken

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Regional Security Assessments: A Strategic Approach to Securing Federal Facilities	5. FUNDING NUMBERS
6. AUTHOR(S) Todd Consolini	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

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

13. ABSTRACT (maximum 200 words)

The 18 critical infrastructure sectors identified by the U.S. Department of Homeland Security form a vast and complex network of interdependent assets that supports the functioning of nearly every aspect of business, government, and commerce. The disruption of even one critical infrastructure sector by a terrorist attack or natural or manmade disaster is likely to have cascading effects on other sectors.

As the Sector-Specific Agency for the Government Facilities Sector, the Federal Protective Service conducts recurring facility security assessments for approximately 9000 federal facilities. These federal facilities are interconnected in varying degrees of complexity and form a network of multi- or bi-directional connections between assets, within or between many types of systems, and within or across critical infrastructure sectors.

This thesis presents a Policy Options Analysis of a cross-sector approach for protecting federal facilities across the United States. These options seek to expand the security assessments conducted by the Federal Protective Service to include interdependency analysis at the operational and strategic levels. These options may also serve as a model for other cross-sector security assessment methodologies that may be adopted by other critical infrastructure sectors.

14. SUBJECT TERMS Federal Protective Service, Policy Option Analysis, critical infrastructure and key resources (CI/KR), interdependency, Facility Security Level, Government Facilities Sector, National Infrastructure Protection Plan (NIPP), risk management	15. NUMBER OF PAGES 103
	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

REGIONAL SECURITY ASSESSMENTS: A STRATEGIC APPROACH TO SECURING FEDERAL FACILITIES

Todd Consolini
Area Commander, U.S. Immigration and Customs Enforcement,
Federal Protective Service, Houston, Texas
B.S., Business Management, University of Phoenix, 2002

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

NAVAL POSTGRADUATE SCHOOL
December 2009

Author: Todd Consolini

Approved by: John Rollins
Thesis Advisor

Rudy Darken
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The 18 critical infrastructure sectors identified by the U.S. Department of Homeland Security form a vast and complex network of interdependent assets that supports the functioning of nearly every aspect of business, government, and commerce. The disruption of even one critical infrastructure sector by a terrorist attack or natural or manmade disaster is likely to have cascading effects on other sectors.

As the Sector-Specific Agency for the Government Facilities Sector, the Federal Protective Service conducts recurring facility security assessments for approximately 9000 federal facilities. These federal facilities are interconnected in varying degrees of complexity and form a network of multi- or bi-directional connections between assets, within or between many types of systems, and within or across critical infrastructure sectors.

This thesis presents a Policy Options Analysis of a cross-sector approach for protecting federal facilities across the United States. These options seek to expand the security assessments conducted by the Federal Protective Service to include interdependency analysis at the operational and strategic levels. These options may also serve as a model for other cross-sector security assessment methodologies that may be adopted by other critical infrastructure sectors.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Federal Protective Service Regional Director Gil Russo and Deputy Regional Director Melissa Shafford for their support and encouragement during my graduate studies. They made it possible to balance work, research, and family time. I would also like to thank John Rollins, Rudy Darken, Mark Harvey, and Pierre Kacha for their guidance, assistance, and feedback during the research and writing of this thesis.

Most of all, I would like to thank my wife, Anjanette, my children Catherine, Vanessa, and Elisabeth, and my granddaughter Jayla for their encouragement and patience during many long hours of research and writing. This thesis and the completion of my graduate studies would not have been possible without them.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THE CRITICAL INFRASTRUCTURE INTERDEPENDENCY NETWORK

The 18 critical infrastructure sectors identified by the Department of Homeland Security (DHS) form a vast and complex network of interdependent assets that supports the functioning of nearly every aspect of business, government, commerce, and life in general. The disruption of even one critical infrastructure sector by a terrorist attack or natural or manmade disaster is likely to have cascading effects on other sectors (Department of Homeland Security [DHS], 2009, pp i, ii, 1). For example, nearly every critical infrastructure sector is dependent on the Energy Sector for electricity, natural gas, and petroleum-based fuels. Nearly every sector requires water and wastewater treatment from the Water Sector. Nearly every sector relies on the Information Technology and Communications Sectors for global voice and data connectivity.

Since none of the critical infrastructure sectors operate in isolation, the question for homeland security professionals is, "Can we adequately protect our critical infrastructure without taking a 'big picture' view across the sectors rather than a sector-specific approach to protection?" This thesis suggests that comprehensive security cannot be provided for the critical infrastructure of the United States without identifying and analyzing interdependent relationships between the 18 critical infrastructure sectors. Such a large-scale, national-level analysis is beyond the scope of this one thesis. However, this thesis does present a policy options analysis of a cross-sector approach for protecting federal facilities across the United States. These options seek to expand the security assessments conducted by the Federal Protective Service (FPS) to include interdependency relationships. These options may also serve as a model for other cross-sector security assessment methodologies that may be adopted by other critical infrastructure sectors.

The term "interdependency" is the most important term for one to understand while reading this thesis and considering the options presented herein. As one will read in the literature review, the terms interdependency and dependency are closely related. Interdependency is defined as the multi- or bi-directional network connections between

assets, within or between systems, and within or across critical infrastructure sectors. For example, a telecommunications network connected to a federal facility is an interdependency because voice and data flow in multiple directions across the network and support the operations of multiple facilities. A dependency refers to a connection that is one-directional (DHS, 2006, pp. 103–104). For example, a water supply is a dependency because the water flows to and is consumed within the facility. While there is a minor distinction between the terms dependency and interdependency, they are so similar that only the term interdependency is used in this thesis for clarity and simplicity. Additional terms related to this thesis are defined in the Appendix at the end of this thesis.

B. PROBLEM STATEMENT

FPS is responsible for the Government Facilities Sector, which is one of the 18 DHS critical infrastructure sectors. FPS conducts recurring facility security assessments for approximately 9000 federal facilities that are under the purview of the General Services Administration (U.S. Immigration and Customs Enforcement [ICE], 2007, p. 2). These federal facilities, along with other critical infrastructure sectors, are interconnected in varying degrees of complexity and form a network of interdependencies. For example, federal facilities operate on electricity and natural gas from the energy sector. Potable drinking water and the disposal of waste water is provided through the water sector. Similarly, information sharing is dependent on infrastructure provided by the communications and information technology sectors and the movement of tangible products is supported by the Postal and Shipping Sector.

The current FPS facility security assessment strategy does not examine this network of interdependencies formed by federal facilities and critical infrastructure sectors and how this network affects the security of federal facilities. Virtually all elements of the current security assessment, including the threat assessment, risk analysis, and countermeasure recommendations, are internally focused on an individual building. Consideration is not given to how the federal facilities are dependent on other critical infrastructure sectors, how the mission of the federal tenant agencies is supported by other federal facilities, or how each facility is impacted by other federal facilities.

Due to the limited scope of these assessments, vulnerabilities that exist in the network formed between federal facilities and critical infrastructure sectors may go unnoticed. The risks associated with these vulnerabilities may not be mitigated and terrorists or criminals may exploit the vulnerabilities. For example, FPS conducts security assessments for the offices operated by the U.S. Department of State's Passport Services Directorate. The Passport Services Directorate has a network of more than 9000 passport acceptance facilities, but there are only 13 Regional Passport Agency offices in the United States that receive, process, and produce passports (U.S. Department of State, 2008). The current FPS security assessment strategy does not adequately address this type of network. Therefore, a criminal or terrorist attack on just one of the 13 regional offices may have a significant global impact on the thousands of passport acceptance facilities and citizens seeking passports.

Another interdependency example is the public water supply system that supports approximately 50 federal facilities in the city of New Orleans. Most of the pipes for the water distribution system were installed 80 to 100 years ago. These pipes are deteriorated and the water pressure in the city is often inadequate. Approximately four times per year federal facilities in the downtown area are closed due to low water pressure (New Orleans Sewage and Water Board, 2006, p. 9). A long-term disruption to the public water supply would effectively close down critical federal operations at agencies such as the U.S. Fifth Circuit Court of Appeals, the U.S. District Court, the U.S. Marshals Service, the Social Security Administration, the Internal Revenue Service, and the Veterans Administration.

C. RESEARCH QUESTION

This thesis examines the policy and process gaps in the current FPS security assessment strategy and answers the following primary research question:

- *How can the Federal Protective Service improve the security of federal facilities by identifying and assessing the network of interdependencies that exists between federal facilities and other critical infrastructure sectors?*

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

- Which interdependencies exist?
- Can these interdependencies be identified?
- Can the identification and assessment of these interdependencies be incorporated into the existing FPS security assessment strategy?
- Which, if any, current FPS strategies or policies support the identification and assessment of interdependencies?
- Can network theory be used to determine the appropriate allocation of security resources?

D. LITERATURE REVIEW

The analysis of critical infrastructure and key resources (CI/KR) interdependencies is rooted in the broad category of infrastructure protection. Federal government policies, directives, and plans, along with scholarly works related to CI/KR, were reviewed for the purpose of addressing the primary and secondary research questions. Both types of literature agree that CI/KR interdependencies exist and their analysis is a critical element of infrastructure protection. The point of difference in the literature is in the solution to this challenge in terms of: whether the analysis should be quantitative or qualitative, whether it should involve complex simulation and modeling or be based on expert analysis and judgment, and the appropriate degree of complexity needed to produce risk data.

1. Federal Government Documents

The first set of literature on this topic consists of federal government documents. They include legislation, directives, strategies, policies, and standards that provide the framework within which the study of CI/KR interdependencies is conducted. The strategies and policies range from federal legislation such as *The Homeland Security Act of 2007* to tactical-level standards such as the *Facility Security Level Determinations for Federal Facilities—An Interagency Security Committee Standard*.

The research question is set within the context of risk management for federal facilities. In particular, the question applies to the mission of FPS with regard to the protection of federal facilities across the country. As a component of DHS, FPS is the primary federal office of responsibility for the Government Facilities Sector-Specific Plan (ICE, 2007, pp. 1, 3–4).

Therefore, the starting point for this literature review is federal documents related to the protection of CI/KR. These documents exist in a hierarchical structure beginning with federal legislation and cascading down through directives, strategies, plans, policies, and standards. The general structure of the federal documents related to this research is shown in Table 1.

Table 1. Hierarchy of Federal CI/KR Documents

	Type of Document	Title of Document
1	Legislation	PL 107–56, Homeland Security Act of 2002
2	Presidential Directive	Homeland Security Presidential Directive 7
3	National Strategy	National Strategy for Homeland Security
4	National Plan	National Infrastructure Protection Plan
5	Sector-specific Plan	Government Facilities Sector-specific Plan
6	Sector-specific Standard	ISC Facility Security Level Determinations for Federal Facilities

The primary federal plan for the protection of CI/KR is the *National Infrastructure Protection Plan* (NIPP). However, one should first understand the broader context of the NIPP and how it fits into the overall strategy for protecting the homeland. This enables the researcher to understand how the network of interdependencies is addressed (or not addressed) throughout the hierarchy of federal homeland security documents. The following sections trace the topic of interdependencies from legislation through sector-specific standards.

a. Homeland Security Act of 2002, Public Law 107-296

The primary purpose of the *Homeland Security Act of 2002* was to establish DHS. While this Act does not specifically use the term interdependencies, it is the primary legislation for directing the protection of the homeland (DHS, 2006, p. 71). Two elements

of the primary mission for DHS provide the basic framework for the protection of CI/KR. Those elements are: (1) reduce the vulnerability of the United States to terrorism; and (2) minimize the damage of and assist in the recovery from terrorist attacks that occur within the United States (U.S. Congress, 2002, p. 8).

There are also statements in the Act from which one can infer that the legislators understood the concept of interdependencies, although they did not use those exact words.

Section 201 (3) reads:

> To *integrate* [emphasis added] relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local Government agencies and authorities, the private sector, and other entities. (United States Congress, 2002, p. 12)

Section 201 (6) reads:

> To recommend measures necessary to protect the key resources and critical infrastructure of the United States *in coordination with* [emphasis added] other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities. (United States Congress, 2002, p. 12)

b. Homeland Security Presidential Directive 7 (HSPD-7)

HSPD-7 lays the foundation for identifying, prioritizing, and protecting CI/KR and led DHS to the development of the NIPP. Like the *Homeland Security Act of 2002*, the terms dependencies and interdependencies are not used in HSPD-7. However, two excerpts show that the writers of HSPD-7 understood the interconnected nature of CI/KR:

- These critical infrastructures and key resources are both physical and cyber-based and *span all sectors* [emphasis added] of the economy" (White House, 2003a, p. 1).

- It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could…have a negative effect on the economy through the *cascading* [emphasis added] disruption of other critical infrastructure and key resources. (White House, 2003a, p. 2)

c. National Strategy for Homeland Security, 2007

The 2007 version of the *National Strategy for Homeland Security* provides an updated framework for protecting the United States. The 2002 version was updated based on five years of countering terrorist threats and the lessons learned from responding to natural disasters such as Hurricane Katrina (Homeland Security Council [HSC], 2007, p. 1). The *Strategy* also makes the protection of CI/KR a key element of homeland security and domestic incident management (DHS, 2006, pp. 71–72).

An interesting point is seen when comparing the 2007 and 2002 versions of the Strategy. In the 2002 version, the protection of CI/KR is not listed in the three overarching strategic objectives. It is listed at the second level of the strategic hierarchy as one of six critical mission areas (Office of Homeland Security, 2002, p. vii). However, in the 2007, version the protection of CI/KR was elevated to one of the four strategic objectives for security of the homeland.

The four goals of the 2007 *Strategy* are:

- Prevent and disrupt terrorist attacks;
- Protect the American people, our critical infrastructure, and key resources [emphasis added];
- Respond to and recover from incidents that do occur; and
- Continue to strengthen the foundation to ensure our long-term success. (HSC, 2007, p. 1)

Within the hierarchy of federal homeland security documents, the *National Strategy for Homeland Security* is the first level where the term "interdependencies" is used:

> While the devastation of even one sector of our critical infrastructure or key resources would have a debilitating effect on our national security and possibly damage the morale and confidence of the

> American people, *interdependencies* [emphasis added] make the protection of CI/KR particularly essential. A failure in one area, such as our water supply system, can adversely affect not only public health but also the ability of first responders to provide emergency services. Accordingly, ensuring the survivability of our CI/KR assets, systems, and networks requires that we continue to accurately model their interdependencies and better assess and understand the potential cascading effects that could impact and impede operations in interconnected infrastructures. (HSC, 2007, pp. 27–28)

> While the Federal government provides overarching leadership and coordination for protecting and mitigating the vulnerabilities of our Nation's CI/KR, all partners in homeland security have important roles to play. Our partnerships also extend to our international neighbors. Many of our CI/KR assets are intertwined with a global infrastructure that has evolved to support modern economies. (HSC, 2007, pp. 28–29)

d. National Infrastructure Protection Plan (NIPP)

The NIPP was written to fulfill the requirements of HSPD-7 and provides an overarching, unified framework for protecting CI/KR across federal, state, territorial, local, tribal, and private sectors (DHS, 2006, pp. i, ii; DHS, 2009, pp. i, iii). The authors of the NIPP identified three specific areas of concern related to interdependencies: cross-sector interdependencies, the cyber dimension, and the international aspect of critical infrastructure. These areas provide more detail about the sub-levels of interdependencies within the national and international network of CI/KR. The first area is cross-sector interdependencies. The NIPP states that the CI/KR sectors form a network of critical functions and directs sector-specific agencies to consider relevant interdependencies when developing sector-specific plans (DHS, 2006, p. 12; DHS, 2009, pp. 9, 17, 21).

The second area of concern in the NIPP is the cyber dimension of interdependencies. The NIPP identifies the global cyber infrastructure as the backbone of the U.S. economy and a critical element of national security (DHS, 2006, p. 13; DHS, 2009, p. 12). It also states that physical CI/KR should not be addressed independent from cyber infrastructure (DHS, 2006, p. 13; DHS, 2009, p. 12).

The third area of concern is international CI/KR protection. The NIPP suggests that the international nature of threats and the global network of CI/KR assets (e.g., energy, transportation, and telecommunications) need special consideration within the risk management and vulnerability analysis framework (DHS, 2006, p. 13; DHS, 2009, pp. 12–13). The specific challenge of protecting international CI/KR is that much of it is outside of the U.S. and not under the control of the U.S. government (DHS, 2006, p. 14; DHS, 2009, pp. 12–13).

Having laid the foundation for understanding the three sublevels of interdependencies, the NIPP then provides a risk management framework within which sector-specific agencies can identify critical vulnerabilities and allocate protection resources to mitigate the highest risk CI/KR (see Figure 1). There are two key factors concerning interdependencies within the NIPP risk management framework:

1. The identification of interdependencies through the National Infrastructure Inventory process. The National Infrastructure Inventory is conducted during Step 2 of the NIPP framework (identify assets, systems, networks, and functions). Interdependencies associated with the CI/KR assets, systems, networks, and functions are documented during this step. (DHS, 2006, pp. 31–32; DHS, 2009, pp. 29–32)

2. The assessment of the interdependencies is conducted during Step 3, which is titled "Assess Risk." (DHS, 2006, p. 37; DHS, 2009, pp. 35–37)

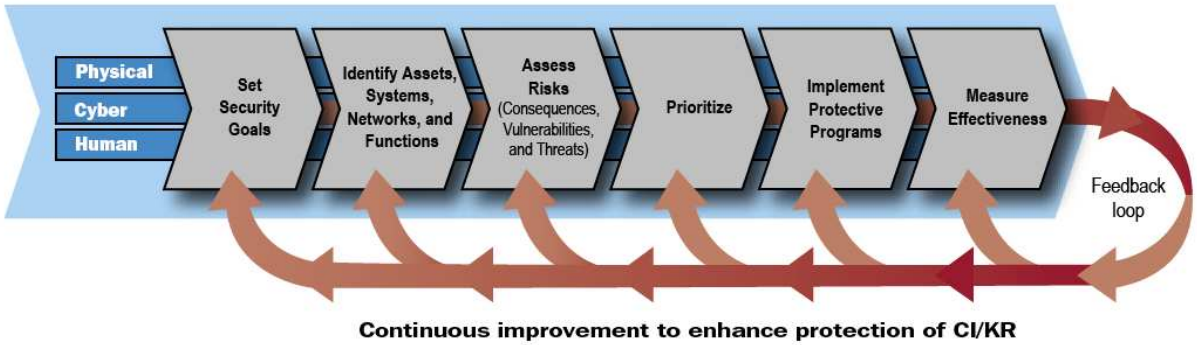

Figure 1. NIPP Risk Management Framework (After DHS, 2006, p. 31; DHS, 2009, p. 27)

From the information presented above regarding the NIPP, one sees that DHS has documented the need to identify and analyze CI/KR interdependencies in the implementation of the national risk

> management framework. The question that must be addressed next is how FPS can accomplish this task. The NIPP suggests two methods: (1) expert judgment or subject matter expertise; and (2) simulation and modeling. (DHS, 2006, p. 37; DHS, 2009, pp. 4, 17, 35)
>
> The expert judgment method involves a simple analysis of interdependencies without the aid of sophisticated software modeling and simulation tools. The outcome yields less detail but might be more practical for many agencies and commercial enterprises. (DHS, 2006, p. 37; DHS, 2009, pp. 4, 17, 35)

The NIPP recommends simulation and modeling tools as a means to comprehensively analyze the impact of interdependencies within a CI/KR sector and across sectors (DHS, 2006, p. 88; DHS, 2009, p. 4). DHS operates the National Infrastructure Simulation and Analysis Center (NISAC), which is specifically charged with providing advanced modeling and simulation capabilities for this purpose (DHS, 2006, p. 37). Additional research will need to be conducted to identify the simulation and modeling tools that may be available from the NISAC.

e. Government Facilities Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan (GF SSP)

The GF SSP presents the application of the NIPP risk management framework to the protection of government facilities (DHS, 2007, p. I). Despite the comprehensive discussion about interdependencies in the NIPP, their analysis in the GF SSP is relegated to an appendix. The authors simply define the term dependency and explain there are four types (physical, cyber, geographic, and logical) (DHS, 2007, p. 97). No specific methodology for identifying and analyzing interdependencies is presented.

f. Facility Security Level Determinations for Federal Facilities—An Interagency Security Committee Standard (FSL Standard)

The FSL Standard is a tactical-level document used by FPS security inspectors to categorize federal facilities according to five equally weighted factors: mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. The FSL determination is based on a scale of one through five. A Level I

building has a lower overall risk rating than a Level V building. Interagency Security Committee (ISC) physical security countermeasure requirements increase as the FSL increases (Interagency Security Committee [ISC], 2008, pp. 5–6).

The only reference to dependencies and interdependencies is in the "Intangible Factors" section of the Standard. FPS security inspectors are encouraged to consider an increase in the FSL for factors that have the potential to impact other facilities and interdependent infrastructure. The security inspector has the discretion to raise or lower the FSL one level (ISC, 2008, p. 13). The risks associated with dependencies and interdependencies are not quantified, analyzed, modeled, or simulated. Instead the GF SSP relies on expert judgment as identified in the NIPP.

2. Scholarly Articles and Books

Scholarly articles and books comprise the second set of literature that may offer a solution to the research question. A review of the federal government documents reveals a gap between acknowledging that CI/KR interdependencies exist and a specific methodology or tool to identify and analyze them. How does network theory apply to the Government Facilities Sector? Are there additional details about interdependencies that can be added and applied to the federal plans and standards? Do modeling and simulation tools exist that can be used specifically for the assessment of federal facilities?

a. Network Theory

The study of interdependencies is rooted in network theory and, more specifically, social network theory. The study of interdependency networks begins with an examination of the basic elements of a small world network and how network theory began. This explains why the interdependency network within the Government Facilities Sector is so important to risk management and the allocation of critical infrastructure protection resources. In his book *Nexus: Small Worlds and the Groundbreaking Science of Networks,* Mark Buchanan explains Stanley Milgram's small world experiments to provide a basic understanding of social network theory. Milgram designed an experiment to learn about the structure of social networks and how the networks are tied together. He mailed 160 letters

through the U.S. Postal Service with the intention of determining the path through which those letters would be delivered. The ultimate destination of all the letters was just one of Milgram's friends. Milgram found that the letters that reached his friend arrived through approximately six steps. He also learned that while the letters followed different paths, all the letters that reached his friend were ultimately routed through just one of three close friends. This simple social network forms the basis of network development and network interdependencies (Buchanan, 2002, pp. 25–26).

Buchanan also explained Mark Granovetter's contribution to social network theory. Granovetter contributed to Milgram's theory by adding that social connections are not all the same. In other words, some connections are stronger than others. Social connections between close friends are strong and tend to include strong ties within a group of friends. On the other hand, some social connections are relatively weak. For example, a connection with an acquaintance is considered to be much weaker than a connection with a close friend. One may assume that the stronger connections between friends and within a group of friends would be more important than relatively weaker connections between acquaintances. Granovetter's research showed this is not necessarily true. The weaker social connections are actually social "bridges" that are critical to forming a social network. In other words, a social bridge is more vital to the network because it connects groups of close friends (e.g., a neighborhood) and reduces the number of steps or hops between people (Buchanan, 2002, pp. 41–43).

The concept of strong and weak links may apply to interdependencies in the Government Facilities Sector. Some interdependency links may be more important than others. For example, the electrical grid may be more important for the operation of federal facilities than the delivery of letters and packages through the U.S. Postal Service. A federal facility can remain operational without postal delivery, but it will be closed due to a lack of electrical power.

Buchanan makes some interesting points regarding both the complexity and simplicity of networks. He cites the work of mathematician Paul Erdos who used mathematics to show the interconnected nature of the global social network. The point that Erdos made is that a small percentage of points in a group can be randomly connected and

the result will be a network that is virtually connected as a whole. In other words, a simple group of unconnected points may easily be formed into an interconnected network with a few random links (Buchanan, 2002, pp. 36–37). Buchanan also suggests that network theory can be used to gain "meaningful simplicity" from inherent complexities. He states that mathematics can be applied to make sense of networks that seem to be too complex for human comprehension (Buchanan, 2002, p. 12).

So how do the writings of Buchanan apply to the study of interdependencies in the Government Facilities Sector? Buchanan himself noted that social network theory can be applied to other non-social puzzles to demonstrate that random links can actually form a network. He used the example of developing a road network that connects towns so a driver may travel between any two towns without leaving the road (Buchanan, 2002, pp. 35–36). In a similar manner, this thesis suggests that the seemingly random network formed within the Government Facilities sector, and the inherent complexities, can be inventoried, analyzed, and possibly modeled to determine a pattern of interdependencies. This pattern or model can then be analyzed and finite critical infrastructure protection resources can be applied according to risk management principles rather than random and/or uninformed decisions.

b. Interdependency Network Characteristics

(1) No unified federal command. The hierarchical organizational structure of the federal government makes the protection of CI/KR in general and federal facilities in particular very challenging. This structure is typically referred to as being "stove-piped," which means that federal agencies operate in isolation and command is focused on vertical linkages, not horizontal linkages. Therefore, there is no one department that is in charge, especially of CI/KR (Lewis, 2006, p. 7). Professor Ted Lewis explains that terrorist networks, in particular al Qaeda, are based on flexible social networking rather than the traditional hierarchical command structure used in the U.S. Within this type of network, called a disintermediated network, data and information move quickly between points in the network; information is easily shared across the entire network, and decisions can be made faster. Lewis contrasts this social network with the inflexible, "stove-piped" federal system

and suggests that poor coordination within the federal command structure produces seams in CI/KR protection, making CI/KR more vulnerable (Lewis, 2006, pp. 7, 12–14).

This characteristic applies to the Government Facilities Sector because federal agencies operate their facilities with little or no coordination when it comes to CI/KR protection. Agencies tend to be concerned only with the security of their particular federal facility without taking into account interdependencies that exist with other facilities or other CI/KR sectors.

(2) Vast and complex. CI/KR in general is a vast and complex network of assets and interdependencies. A brief list of CI/KR statistics provides one with a sense of the magnitude and complexity. Within the U.S. there are approximately:

- 2,800 power plants
- 300,000 production sites for oil and natural gas
- 5,000 airports
- 120,000 miles of major railroads
- 590,000 highway bridges
- 26,600 FDIC insured banking institutions
- 66,000 chemical plants
- 104 commercial nuclear power plants
- 80,000 dams. (White House, 2003b, p. 9)

(3) Random, scale-free, and small world. Buchanan's explanation of Milgram's social networking experiments showed that seemingly random elements may in fact form a network (Buchanan, 2002, pp. 25–26). This theory can be applied to the study of interdependencies in the Government Facilities Sector. In a sense, the location of federal facilities and how they fit into the infrastructure network appears to be quite random when viewed across all federal departments and agencies. Federal agencies do not necessarily collaborate with one another when they select a particular facility in which to conduct their operations. They typically select their location and infrastructure linkages based on their

individual requirements. The application of Buchanan's and Lewis's theories may show that the federal facilities network may not be so random. Applying network theory may actually show that federal facilities form a scale-free network (a small number of hubs formed by a high concentration of links) or a small-world network (clusters of nodes) (Lewis, 2006, pp. 82–92).

c. Additional Interdependencies

Yacov Haimes suggests additional interdependencies that are not addressed in the federal documents. For example, he identifies human, social, and organizational infrastructure elements (Haimes, 2002, p. 38).

Human and social interdependencies exist within the Government Facilities Sector and should not be overlooked. After all, the primary work of the federal government is social. The preamble to the *Constitution of the United States* supports this claim. The *Constitution* was written to "establish justice, insure domestic tranquility, provide for the common defense, promote general welfare, and secure the blessings of liberty to ourselves and our posterity…" (U.S. Government Printing Office, 2007, p. 1). Therefore, human and social interdependencies should be considered within the Government Facilities Sector.

One should also consider the behaviors and perceptions of humans within the Government Facilities Sector as part of the human and social interdependencies. Howard Kunreuther suggests that security issues related to interdependencies can be viewed from an individual perspective and a social perspective, and the two are likely to meet in relation to interdependencies (Kunreuther, 2007, p. 3). He hypothesizes that two equilibriums exist in the protection of interdependencies. Either everyone invests in interdependency protection or no one does. Kunreuther explains that if one person or organization invests in interdependency protection then others are more likely to so (Kunreuther, 2007, p. 3). The opposite may also be true in that if one person or organization does not invest in protection then others will not either (Kunreuther, 2007, p. 3).

Kunreuther's theory may apply to the Government Facilities Sector. Federal agencies may look at the security practices and behaviors of other agencies and make risk management decisions based on perception. An example of this is the U.S. Postal Service.

Many federal agencies rely on the U.S. Postal Service to screen mail and packages prior to delivery. These agencies have a perception that they are protected. But is this true? Is their perception driven by a false understanding of U.S. Postal Service security practices? Would they not be more secure if they understood the actual screening process and ensured their mail and packages are screened according to their own risk analysis?

Organizational interdependencies exist in a network formed by federal agencies, departments, and subdivisions. Federal organizational elements share information and intelligence and provide products and services to other federal entities. An example of a federal organizational interdependency is the work performed by the General Services Administration (GSA). Many federal agencies depend on GSA for real estate, engineering, and building maintenance services. The loss or degradation of GSA services due to a terrorist attack or security incident may have a far-reaching impact on other federal organizations.

The necessity of identifying and analyzing information technology (IT) interdependencies is emphasized by Chittester and Haimes. CI/KR are interconnected through IT systems such as supervisory control and data acquisition systems, global positioning systems, satellites, intranets, and the Internet (Chittester and Haimes, 2004, p. 1). IT plays a significant role in the successful operation of federal facilities and for the agencies housed in those facilities. In fact, the degradation of federal IT systems has a significant negative impact on the services provided by federal agencies. Therefore, IT interdependencies should be addressed in any Government Facilities Sector risk methodology.

Human, social, organizational, and IT interdependencies could be added to the list of interdependencies examined in the NIPP and GF SSP to expand the scope of the risk management framework.

3. Conclusion

Federal documents within the CI/KR hierarchy express the *need* to identify and analyze interdependencies; however, none of them provide guidance or policy about how this will be accomplished. For FPS specifically, the NIPP and GF SSP call for the

identification and analysis of interdependencies within the DHS risk management framework, but both documents leave a gap in how these actions should be accomplished. DHS suggests the use of expert judgment and modeling and simulation as the general methods for interdependency analysis. However, as the Government Facilities Sector-Specific Agency, FPS does not currently use modeling and simulation and the use of expert judgment is questionable given the lack of a specific methodology in the GF SSP.

E. ARGUMENT

This thesis recommends a more strategic approach for assessing the security of federal facilities. Rather than focusing exclusively on the assessment of a single federal facility in isolation, FPS should develop a regional security assessment strategy that accounts for interdependencies and interdependency networks. Such a strategy would be used to identify and model the interdependency network across a selected geographic region. This approach begins with interdependency identification and data collection at the tactical level. This data would then be used by FPS security managers working at the operational and strategic levels of the organization to model and analyze the interdependency network and determine how to appropriately allocate finite security resources.

The literature review identified that current federal government documents related to the protection of federal facilities call for considering interdependencies as a factor in the DHS risk management process. These documents provide a framework within which a regional security assessment strategy would fit. However, none of the documents, including the tactical-level standards used by FPS, provide a methodology for doing so. A detailed analysis of federal policy was conducted to determine which FPS policies need to be modified to incorporate a regional security assessment strategy and which policies support such a strategy. As the Government Facilities Sector-Specific Agency and a member of the Interagency Security Committee, FPS cannot make unilateral policy changes. Therefore, the details of the regional security assessment strategy include specific recommendations for

modifying selected federal policies and standards within the current framework. The recommended strategies fit within the current GF SSP and NIPP frameworks and support the use of the DHS risk management framework.

F. SIGNIFICANCE OF THE RESEARCH

This research is significant for FPS because it shows the importance of interdependency analysis and presents realistic and appropriate policy revisions to address the risks that may be associated with interdependencies. The proposed policy recommendations seek to achieve two specific goals. The first goal is to fill the policy gap in the identification and analysis of interdependencies that begins in the GF SSP and cascades down through FPS policies and directives. The second goal is to recommend a more strategic approach to FPS security assessments and risk management by adding strategic- and operational-level security analyses.

The immediate customer for this research is the Risk Management Division of FPS. The division director may approve, disapprove, or modify the policy recommendations that are made in this thesis. If approved by the division director, the policy recommendations may be published by the FPS director in the form of an agency-wide directive and would be incorporated into the physical security training program. Ultimately FPS security inspectors and regional managers across the United States would utilize the new policies to incorporate the identification and analysis of interdependencies into the building security assessment process. Additionally, FPS stakeholders who rely on these security assessments would be able to make better informed decisions on how best to apply their finite security resources to adequately protect their facilities.

Future research related to this topic should focus on elevating interdependency analysis to the national level for FPS. This thesis recommends a regional-level perspective (i.e., a relatively large and well-defined geographic area) as an initial means to move beyond the current building-centric perspective. The interdependency network actually extends beyond the regional level and security at multiple federal facilities may be affected by interdependencies that reach across the country or around the world.

G. METHODOLOGY

The Policy Options Analysis method used for this thesis is based on the "Eightfold Path" presented by Eugene Bardach in his book titled, *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving*. The following policy analysis steps were adopted from Bardach's path: (1) define the problem; (2) assemble some evidence; (3) construct alternatives; (4) select the criteria; (5) project the outcomes; and (6) decide (Bardach, 2005, p. xiv). Bardach's other two steps, "confront the trade-offs" and "tell your story" were incorporated into the other six steps for this thesis.

The problem statement originated from the thesis author's experience with conducting, reviewing, and evaluating FPS Building Security Assessments over a three and a half year period. The problem statement was refined and validated by comparing the current FPS security assessment strategy to the interdependency analysis requirements contained in federal infrastructure policies and plans. The literature review was used to gather evidence related to this topic and to develop the options presented in this thesis for solving the primary and secondary research questions. Evaluation and selection criteria were developed based on the research conducted during the literature review. The anticipated outcomes of each alternative were developed based on rating each alternative against the evaluation criteria. The final outcome is the decision step in which the best policy alternative was determined and future steps were outlined.

H. CHAPTER OVERVIEW

Chapter II presents an analysis of the current FPS security assessment strategy. Maintaining status quo means that FPS security inspectors would continue to use their discretion in identifying and analyzing interdependencies. In particular, this relies on the "Intangible Factors" section of the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard* as the primary means through which interdependencies will be considered during the security assessment process.

Chapter III addresses modifying the current FPS building security assessment process. FPS Directive 07-004, *Building Security Assessment Program*, would be modified

to require the identification and analysis of interdependencies. FPS security inspectors would identify 10 common interdependencies in accordance with the *National Infrastructure Protection Plan* and the *Government Facilities Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*. Inspectors would then use expert analysis, as described in the NIPP, to determine the risk associated with the interdependencies.

Chapter IV suggests modifying the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard*. This option would require the inclusion of interdependencies when calculating the security level of each federal facility. Rather than being an optional consideration, interdependencies would be the sixth element of the security level calculation along with mission criticality, symbolism, facility population, facility size, and threat to tenant agencies (ISC, 2008, pp. 4–13).

Chapter V suggests developing a comprehensive regional security assessment strategy. The purpose of a regional security assessment strategy would be to meet the full intent of the NIPP Risk Management Framework, which is to identify interdependencies and then analyze them using modeling and simulation (DHS, 2006, pp. 31–32, 37). The outcome would be a regional security assessment that would be used to direct the allocation of finite security resources across a broad strategic area.

Chapter VI presents an analysis of the four policy options and each policy option is evaluated using five criteria: compliance with standards, effectiveness, implementation, institutional acceptability, and time investment. Chapter VI also suggests the best policy option based on the five criteria and presents future work related to the best option.

II. ANALYSIS OF THE CURRENT FPS SECURITY ASSESSMENT STRATEGY

The current FPS security assessment strategy relies on two elements related to identifying and analyzing interdependencies: increasing the Facility Security Level if interdependencies impact the security of a federal facility and identifying public utilities for the building being assessed. Both elements rely on expert analysis carried out by FPS security inspectors.

A. INCREASING THE FACILITY SECURITY LEVEL

One of the first steps in the FPS security assessment is to calculate a Facility Security Level for a particular federal facility. This calculation may be completed as early as the initial building or space identification and should be made early enough to accommodate installation and implementation of appropriate security measures. A Facility Security Level is a numerical categorization that is used to determine the appropriate security countermeasures that should be implemented for an individual federal facility (ISC, 2008, pp. 1–3).

The final Facility Security Level determination is based on a scale of one through five. On the lower end of the scale, a Level I building is characterized as having a mission that is not necessarily essential or vital for the functioning of the federal government, does not present a symbolic target to criminals and terrorists, has a population of less than 100 people, is less than 10,000 square feet in occupied space, and has a low threat rating (ISC, 2008, pp. 7–13). A small office space in a rural town used by the U.S. Census Bureau is an example of a Level I facility.

At the upper end of the scale, a Level IV building is characterized as having a mission that is considered to be a National Essential Function. The building is very symbolic of the federal government and is, therefore, an attractive target; has a population of more than 750 people; is greater than 250,000 square feet of occupied space; and has a high threat rating (ISC, 2008, pp. 7–13). A large Internal Revenue Service office that services a large population in a major metropolitan area is an example of a Level IV facility.

Facility Security Levels II and III fit within the scale between the Level I and Level IV facilities. A Level V facility is one that requires protection greater than that provided for a Level IV facility because of unique factors that are not accounted for in the standard Facility Security Level calculation. For example, a facility may be the only one in the United States that provides a particular service or product to the federal government and, therefore, requires additional security measures to protect it. A facility may also be highly symbolic and a very attractive target for terrorists and criminals. The White House, the headquarters for the Central Intelligence Agency, and the headquarters for the Department of Homeland Security are examples of Level V facilities (ISC, 2008, p. 14).

The Facility Security Level calculation is based on five equally weighted security factors. These factors are mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. Each factor is assigned a score of one through four based specific criteria presented in the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard*. The scores assigned to each factor are added to produce a preliminary Facility Security Level (ISC, 2008, pp. 5–6).

A sixth, non-weighted security factor, called an "Intangible Factor," is then used to take into consideration special circumstances or conditions that may not be accounted for in the five equally weighted factors. The FPS security inspector may use expert judgment and analysis to increase the Facility Security Level a maximum of one level due to interdependencies (ISC, 2008, pp. 5, 13). Table 2 provides an overview of the five factors and how the current Facility Security Level is calculated.

Table 2. ISC Facility Security Level Determination Matrix (From Interagency Security Committee, 2008, p. 6.)

Factor	Points				Score
	1	2	3	4	
Mission Criticality	LOW	MEDIUM	HIGH	VERY HIGH	
Symbolism	LOW	MEDIUM	HIGH	VERY HIGH	
Facility Population	< 100	101–250	251–750	> 750	
Facility Size	< 10,000 sq. ft.	10,001–100,000 sq. ft.	100,001–250,000 sq. ft.	> 250,000 sq. ft.	
Threat to Tenant Agencies	LOW	MEDIUM	HIGH	VERY HIGH	
					Sum of above
Facility Security Level	**I** 5–7 Points	**II** 8–12 Points	**III** 13–17 Points	**IV** 18–20 Points	Preliminary FSL
Intangible Adjustment	Justification				+ / - 1 FSL
					Final FSL

B. IDENTIFYING PUBLIC UTILITIES

The FPS security assessment methodology is called the Building Security Assessment Program. Software called FSR-Manager supports the security assessment process and the writing of the Building Security Assessment. The only element within the Building Security Assessment Program and FSR-Manager methodologies that considers interdependencies is contained in the section of the security assessment titled "Description of the Facility." In this section, the FPS security inspector is required to identify and document the public utility providers of electricity, natural gas, and water. The only

information provided is the name and telephone number of the public utility that provides the particular service. The inspector is not required to assess the vulnerabilities, levels of risk, and impact of loss associated with these utilities (Applied Research Associates, Inc., 2001, p. 2–17).

C. ASSESSMENT AGAINST EVALUATION CRITERIA

Each policy option presented in this thesis was assessed using five evaluation criteria. These criteria are compliance with standards, effectiveness, implementation, institutional acceptability, and time. Table 3 summarizes the assessment of the current FPS Building Security Assessment Strategy against these criteria. An explanation of the criteria is provided after the table to facilitate understanding.

Table 3. Table 3 Evaluation Criteria Matrix for Option I

Option	Compliance with Standards	Effectiveness	Implementation	Institutional Acceptability	Time
I	Non-compliant	Low	Simple	High	No investment

D. POLICY OPTIONS EVALUATION CRITERIA

The policy options presented in this thesis were evaluated according to the following rank-ordered criteria that are defined below: compliance, effectiveness, implementation, institutional acceptability, and time investment.

Compliance with standards is the degree to which the option complies with the NIPP and fits within the NIPP risk management framework. This criterion is rated as compliant, partially compliant, or non-compliant. Compliant means the solution conforms to the full intent of the 2009 NIPP risk management framework. Partially compliant means the solution conforms to only part of the 2009 NIPP risk management framework and requires modification to reach compliance. Non-compliant means the solution does not, in any manner, conform to the 2009 NIPP risk management framework.

Effectiveness is the anticipated degree of overall risk reduction associated with assessing interdependencies. This criterion is rated as high, medium, or low levels of risk reduction. A high level of risk reduction means the solution will improve the security of multiple federal facilities because interdependencies are factored into the assessments. A medium level of risk reduction means the solution will improve the security of one federal facility because interdependencies for that particular facility will be factored into the assessments. A low level of risk reduction means the solution provides minimal or no improvement in the security of a federal facility because interdependencies are not factored into the assessments.

Implementation is the relative ease with which the option can be implemented across the FPS. This criterion is rated as very difficult, moderately difficult, or simple. A very difficult rating means the solution will require the revision of more than two FPS policies and a major revision of FPS physical security training programs. A moderately difficult rating means the solution will require the revision of no more than two policies and conducting the associated training. A simple rating means the solution will require virtually no policy revision and training.

Institutional acceptability is the anticipated degree of acceptance across all organizational levels of FPS. An acceptability rating of high means the solution is expected to be readily accepted by all FPS security managers and inspectors. An acceptability rating of medium means the solution is expected to be readily accepted by FPS security managers, but not readily accepted by the security inspectors who conduct the assessments. An acceptability rating of low means that the solution is not expected to be readily accepted by any FPS security managers and inspectors and a high level of demonstration will be required to gain full acceptance.

Time investment is the amount of time necessary to bring the solution to full development and implementation within FPS. This criterion is rated as major time investment, minor time investment, or minimal time investment. A major time investment means development and implementation are expected to take more than two years. A minor time investment means development and implementation are expected to take more than six

months but less than two years. A minimal time investment means development and implementation are expected to take less than six months.

1. Compliance with Standards

The current FPS Security Assessment Strategy does not comply with the NIPP and the NIPP risk management framework. While the NIPP does not provide a specific methodology for identifying and analyzing interdependencies, it does direct sector-specific agencies, including interdependencies in their risk assessments. In particular the NIPP recommends that interdependencies should be inventoried during the "Identify Assets, Systems, and Networks" step of the risk management framework (DHS, 2006, pp. 12, 31–32, 37; DHS, 2009, pp. 9, 17, 21, 29–32, 35–37). The NIPP also recommends that those interdependencies should be analyzed using expert judgment or modeling and simulation during the "Assess Risks" step of the framework (DHS, 2006, pp. 12, 31–32, 37; DHS, 2009, pp. 9, 17, 21, 29–32, 35–37). As the Sector-Specific Agency for Government Facilities, FPS also briefly identifies the need to identify and analyze interdependencies in the *Government Facilities Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan (GF SSP)* (DHS, 2007, p. 97). Neither the direction from the NIPP nor the GF SSP is incorporated into the current FPS strategy because this strategy preceded both the NIPP and the GF SSP. The first version of the NIPP was published in 2006, and the GF SSP was published in 2008. Development of the 2007 Building Security Assessment Program was primarily based on the security assessment methodology presented in the 2001 FSR-Manager software. Therefore, it is not difficult to determine that non-compliance with the NIPP interdependency assessment is due to the publication sequence of these documents rather than neglect of the issue on the part of FPS.

2. Effectiveness

The current strategy is assessed as having a low level of effectiveness in terms of reducing the risks associated with interdependencies. As noted previously,

interdependencies are not adequately identified and, therefore, are not assessed. Therefore, the risks associated with interdependencies cannot be properly determined.

3. Implementation, Institutional Acceptability, and Time

Implementation is assessed as simple, institutional acceptability is rated as high, and time investment is rated as minimal. These ratings are appropriate because the current Building Security Assessment Program has been in use since 2007 and most of that methodology, with some minor revisions, has been in use since 2001. Policy revision and additional training are not required for maintaining status quo and the current strategy is already accepted by most FPS security managers and inspectors. There is no time required for development and implementation.

E. OVERALL ASSESSMENT

The current Facility Security Level and Building Security Assessment methodologies do not adequately address the impact of interdependencies on the security of federal facilities.

First, the risks associated with interdependencies are not quantified and weighted equally with the five primary factors in the Facility Security Level calculation. Interdependencies are one of many factors that may be considered under the "intangible factors" in the Facility Security Level calculation. Instead the calculation relies on expert judgment on the part of FPS security inspectors.

The Facility Security Level calculation instructions incorrectly assume that FPS security inspectors can apply expert judgment for identifying interdependencies, including their impact on security in the "intangible factors," and appropriately determine if the Facility Security Level should be increased a maximum of one level due to risks associated with interdependencies. FPS security inspectors receive no education or training in identifying and analyzing interdependencies while attending the FPS Physical Security Training Program or during on-the-job training. Field experience of the thesis author has shown that FPS inspectors do not know how to properly identify interdependencies and properly assess whether the Facility Security Level should be increased.

Even if FPS inspectors were trained to appropriately increase the Facility Security Level for a particular facility based on risks associated with interdependencies, the Building Security Assessment that is conducted following the Facility Security Level calculation does not support interdependency identification and analysis and the implementation of appropriate security countermeasures. Simply identifying the providers of electricity, natural gas, and water is not enough for effective interdependency assessment.

Maintaining status quo is presented in this thesis as Option I for the purposes of evaluating it against the evaluation criteria and comparing it against other options to determine the best policy option for FPS.

III. OPTION II: MODIFY THE FPS BUILDING SECURITY ASSESSMENT PROGRAM

A. OVERVIEW OF OPTION II

Option II recommends modifying the FPS Building Security Assessment Program to include the identification and analysis of interdependencies. FPS Directive 07-004, *Building Security Assessment Program*, would be modified with additional steps to require the identification and analysis of interdependencies. FPS security inspectors would identify 10 common interdependencies in accordance with the *National Infrastructure Protection Plan* and the *Government Facilities Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*. FPS security inspectors would then use expert analysis, as described in the NIPP, to determine the risks associated with the interdependencies.

Within the context of this thesis, the term "expert analysis" is defined as an analysis that is conducted by one who has special knowledge about a particular subject. This knowledge is considered to be above that which the average person would normally possess. Such a person may also be referred to as a subject matter expert and usually possesses education, credentials, or experience that can be verified and that qualify the person to be considered an expert (U.S. Legal, Inc., 2009). FPS security managers and inspectors could be considered subject matter experts for the assessment of the security of federal facilities. They receive formal education and training in the Building Security Assessment Program, receive federal credentials that certify them as Law Enforcement Security Officers, and engage daily in assessing the security of federal facilities. They are well-suited and prepared to learn and implement the specific elements of Option II.

The general intent of Option II is to incorporate the identification and analysis of interdependencies within the current FPS security assessment framework. This presents FPS with an option that does not require a major revision of the security assessment framework and methodology, takes a relatively short amount of time to implement, and will not require extensive training for FPS security managers and inspectors.

This option also intends to follow guidance provided in the NIPP that suggests expert judgment is an appropriate means for assessing interdependencies. The writers of the NIPP acknowledged that the sophistication and level of detail provided by modeling and simulation may not be practical or necessary. Therefore, expert judgment may provide an appropriate level of data in order to make risk management decisions (DHS, 2009, p. 35). This option presents such an alternative to modeling and simulation.

Option II also follows NIPP guidance about tailoring risk management methodologies that apply to the specific assets within a critical infrastructure sector. The NIPP suggests that the best approach to assessing fixed assets and physical facilities, such as federal facilities, may be a bottom-up, asset-by-asset approach (DHS, 2009, pp. 27–28). This option exploits the current facility-centric security assessment approach and adds the interdependency identification and analysis steps to the process.

Option II involves incorporating elements of steps two through five of the NIPP risk management framework into the FPS Building Security Assessment process (see Figure 2). These steps are "Identify Assets, Systems, and Networks," "Assess Risks," "Prioritize," and "Implement Protective Programs" (DHS, 2006, pp. 12, 31–32, 37; DHS, 2009, pp. 9, 17, 21, 29–32, 35–37).

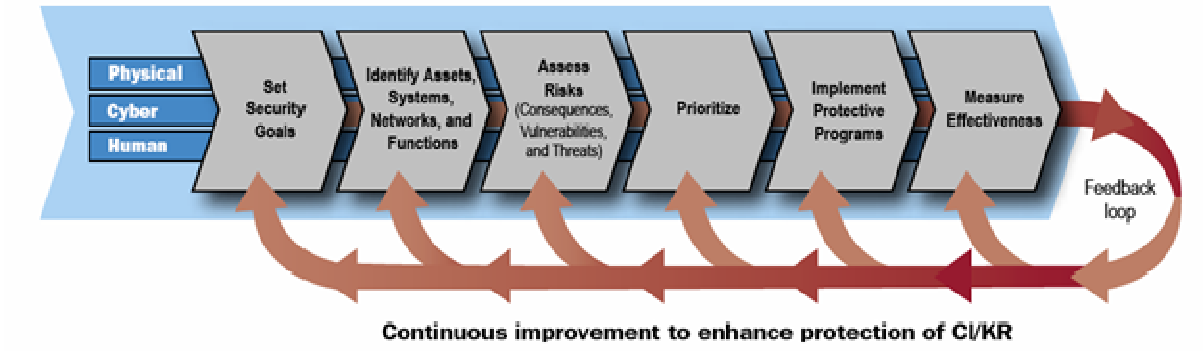

Figure 2. NIPP Risk Management Framework (After DHS, 2006, p. 31; DHS, 2009, p. 27)

B. DETAILS OF OPTION II

The following sections provide the details of Options II and the recommended modifications to the FPS Building Security Assessment process. In general, FPS security inspectors would inventory 10 common interdependencies as part of the current inventory process, gather data related to these interdependencies, analyze threats related to the interdependencies and calculate risk ratings according to existing FPS criteria, and make countermeasure upgrade recommendations using the current process.

1. Step 1: Inventory Interdependencies

The inventory of interdependencies would be completed during the initial data collection step of the current security assessment process. The FPS security inspector currently inventories the federal facility and documents information such as the locations and types of entrances and exits, mail and package delivery and processing procedures, parking in and around the facility, and neighboring facilities (Applied Research Associates, 2001, p. 2–21).

Option II recommends adding 10 common interdependencies and associated data in the existing "Facility Specific Details," "Optional Topic" section of the FSR-Manager software data fields (see Figure 3). The suggested interdependencies with associated definitions are listed in Table 4. The FPS security inspector should describe how the interdependency relates to the facility, in as much detail as possible, in the "Description" field in FSR-Manager. This description should include the capabilities provided to the facility by the interdependency, links within the facility and with other facilities, and the consequence cost to the tenants in terms of interdependency failure or replacement (Lewis, 2006, p. 110).

The 10 interdependencies and the associated descriptions will be automatically transferred to and documented in the "Description of the Facility" section of the Building Security Assessment as part of the data output from the FSR-Manager software. The FPS security inspector can then use this information when making expert judgments during the risk rating step in the current security assessment process.

Table 4. Common Interdependencies for Federal Facilities

Interdependency	Definition
Electrical Power	Primary and backup electrical power sources
Natural Gas Supply	Primary natural gas supply
Water Supply	Primary water supply
Waste Water Disposal	Primary wastewater disposal system
Communications	Voice services provided from or utilized by federal tenant agencies. These include terrestrial, satellite, and wireless transmission systems (DHS, 2009)
Information Technology	Hardware, software, and IT systems provided or utilized by federal tenant agencies. This includes all classified and unclassified Internet connections provided or utilized by federal tenant agencies (DHS, 2009)
Postal Service	Small- and medium-size packages delivered and retrieved by the U.S. Postal Service (DHS, 2009)
Shipping Services	Small- and medium-size packages delivered and retrieved by the commercial courier services (DHS, 2009)
Organizational Connections	Sharing of information, intelligence, products or services within and between organizational elements
Human and Social Factors	Human and social behaviors that exist within the facility and between facilities and should be considered from a security perspective

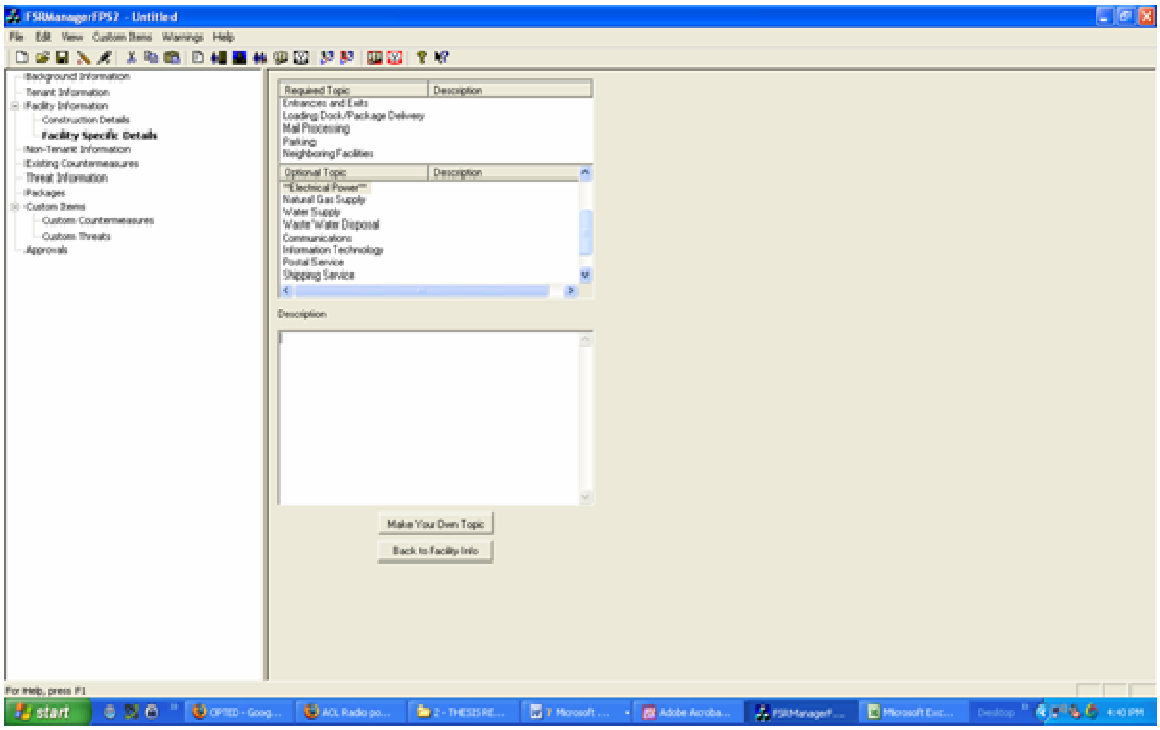

Figure 3. Screen Shot of Facility Specific Details Page in FSR-Manager

2. Step 2: Analyze Interdependencies

The analysis of the 10 common interdependencies would be completed during the risk rating step in the current FPS security assessment process. Using the current process, the FPS security inspector conducts a threat-based risk assessment that is described below.

The inspector begins by rating each threat that was identified during the data collection phase of the process using two categories. The first category is impact of loss, which is defined as the "degree to which the mission of the tenant(s) is impaired by a successful attack from the given threat." High, moderate, and low impact of loss ratings are assigned to each threat according to the following criteria:

- High: "Complete loss of assets/mission capability or extreme impairment of mission capability is expected for an indefinite period of time."
- Moderate: "Noticeable impact of mission capability or loss of major assets is expected for a limited period of time."

- Low: “No noticeable impact on mission capability or loss of major assets is expected.” (Applied Research Associates, 2001 pp. 2-32, 2-33)

The second category is vulnerability, which is defined as “a combination of the attractiveness of a facility as a target and the level of deterrence and/or defense provided by the existing countermeasures.” High, moderate, and low vulnerability ratings are assigned to each threat according to the following criteria:

- High: “The facility is an attractive target, and the existing countermeasures are providing little or no deterrence and/or defense.”
- Moderate: “The facility is an attractive target, and the existing countermeasures are providing a moderate level of deterrence and/or defense.”
- Low: “The facility is not an attractive target, and the existing countermeasures are providing a high level of deterrence and/or defense.” (Applied Research Associates, 2001, p. 2-33)

The final step in the risk rating process is to determine a combined risk rating for each threat using the previously assigned impact of loss and vulnerability ratings. This is accomplished by using Tables 5 and 6 that show how to determine each rating.

Table 5. Combined Risk Ratings (From Applied Research Associates, 2001, pp. 2-33, 2-34)

Matrix for Risk Ratings

	Vulnerability to Threat		
Impact of Loss	High	Moderate	Low
High			
Moderate			
Low			

Table 6. Explanation of Risk Ratings (From Applied Research Associates, 2001, pp. 2-33, 2-34)

Explanation of Risk Ratings	
	These risks are high. A countermeasure must be implemented to mitigate high risk threats.
	These risks are moderate. Countermeasure implementation is at the discretion of the Building Security Committee and tenant agencies.
	These risks are low. Countermeasure implementation is at the discretion of the Building Security Committee and tenant agencies.

Option II suggests adding steps to the analysis process in order to properly assess the security vulnerabilities that may exist due to interdependencies. The FPS security inspector gathered pertinent interdependency data during the inventory phase of the security assessment. At this point in the assessment process, the FPS security inspector should be able to answer the following questions regarding the 10 common interdependencies:

- What capabilities are provided to the facility by the interdependency?
- What links exist within the facility and with other facilities?
- What consequence costs are there to the tenants in terms of interdependency failure or replacement? (Lewis, 2006, p. 110)

Within the current FPS Building Security Assessment Program and FSR-Manager frameworks, the answers to these interdependency questions should provide enough information for the FPS security inspector to make an expert judgment regarding the security threats that may be present due to one or more of the interdependencies. For example, the inventory and analysis may show that critical telecommunications equipment in the facility that must operate at all times to support operations external to the facility is not connected to any type of electrical backup power system and the electrical power supply may not be adequately protected by the commercial electric provider. The costs of electrical power failure in terms of lose of mission capability and continuity of operations may far exceed the cost of installing a backup electrical power generator.

Another example is that a review of organizational connections may reveal that the facility is a one-of-a-kind center or one-of-a-few centers for producing a specific product on behalf of the federal government. This is the case with passport production offices throughout the United States. The cost of a successful attack on such a facility in terms of delays in production and duplicating the work effort at another location may far exceed the cost of adequate security countermeasures.

The FPS security inspector should then use the current threat-based risk assessment process previously described in this chapter to analyze potential threats to the interdependencies. This includes assessing the impact of loss if there were a successful attack on the interdependency and the vulnerability of the interdependency to the threat. Using the previous electrical power failure example illustrates this process.

An FPS security inspector may find during the inventory that a facility does not have a backup electrical power system. By using the steps suggested in Option II, the inspector may find that the critical telecommunications equipment in the facility supports agencies who do not occupy the facility and they may not be aware that their critical equipment will not function if there were to be an electrical power outage. By calculating the consequence costs related to the failure or replacement of the telecommunications equipment, the FPS security inspector may determine that the loss of electrical power to the facility is a threat. Table 7 shows what this risk analysis would look like in the current Building Security Assessment format.

Table 7. Interdependency Threat Example

Current Threat Ratings			
Threat	Impact Of Loss	Vulnerability	Combined Risk
Loss of Electrical Power	Moderate	Moderate	Moderate

Table 8 shows how the FPS security inspector would justify the loss of electrical power to the facility as a credible threat using the current FPS Building Security Assessment Program and the FSR-Manager software.

Table 8. Credible Threats Example

Credible Threats for this Facility	
Threat	Justification—Why Credible
Loss of electrical power to the facility	Loss of electrical power would cause a failure of the communications equipment for agencies housed in this facility and for operations at X number of other facilities. The cost of loss of mission capability is expected to be X number of hours and X number of dollars.

3. Steps 3 and 4: Prioritize and Implement Protective Programs

During the next step in the process, the FPS security inspector uses the overall risk ratings to develop countermeasure recommendations for the facility being assessed. These countermeasures are prioritized and implemented according to mandatory and optional categories. A mandatory countermeasure is defined as one that mitigates a high-risk threat and an optional countermeasure mitigates a moderate- or low-risk threat. Both types of countermeasures must meet minimum standards set forth by the Interagency Security Committee, the Department of Justice, or a nationally recognized security standard. After completing the security assessment, the FPS security inspector presents the overall risk ratings and the countermeasures to representatives from the tenant agencies and they decide which countermeasures they are willing to fund and implement (Federal Protective Service, 2007, p. 8). The FSR-Manager software automatically suggests countermeasures based on the data input. Table 9 lists the possible countermeasures from which the FPS security inspector may choose for the mandatory and optional countermeasures. The FPS security inspector may add custom countermeasures into the assessment as long as the countermeasures meet the minimum standards referenced above.

Table 9. Master List of Suggested Security Countermeasures from FSR Manager

MASTER LIST OF COUNTERMEASURES
Air Intake Access Control
Awareness Training
Closed-Circuit Television
Chemical Agent Detection
Crime Prevention Through Environmental Design
Duress Alarms
Electronic Access Control
Emergency Power Source
Employee ID System
Fencing
Guard Training
Guards
HVAC Access Control
Intecom
Key Control
Locks
Magnetometers
Mantraps
Occupant Emergency Plan
Perimeter Alarm System/Intrusion Detection System
Perimeter Lighting
Perimeter Patrol
Restricted Perimeter Parking
Shipping/Receiving Procedures
Signage
Vehicle Barriers
Vehicle Inspection
Visitor ID System
Water Supply Access Control
Window Protection
X-Ray Mail Screening
X-Ray Visitor Screening

Option II suggests the use of the same process for prioritization and implementation of security countermeasures. The FPS security inspector would use the data from the risk ratings analysis and determine appropriate security countermeasures based on the criteria that are listed the previous paragraph. Using the electrical power failure example, Table 10 shows what this countermeasure recommendation would look like in the current Building Security Assessment format.

Table 10. Interdependency Countermeasure Recommendation

Countermeasure Upgrade Descriptions		
Package Name	Countermeasure	Description
Optional Package	Backup electrical power generator	A backup electrical power generator should be installed to operate the critical communications equipment in this facility. The generator should be capable of providing X number of kilowatts of electricity for X number of hours.

The final step in the current FPS Building Security Assessment process is to determine the projected combined risk rating if the recommended countermeasure is implemented. The FPS security inspector uses expert judgment to determine the anticipated change in impact of loss and vulnerability ratings, which then provide the projected combined risk rating. The objective is to show that the recommended countermeasure will result in a lower combined risk rating and, therefore, should be implemented. Table 11 shows how the installation of a backup electrical power generator might lower the combined risk of the threat of electrical power loss.

Table 11. Projected Threat Ratings Example

Projected Threat Ratings After Upgrades				
Package Name	Threat	Impact Of Loss	Vulnerability	Combined Risk
Optional Package	Loss of electrical power	Low	Moderate	Low

C. ASSESSMENT AGAINST EVALUATION CRITERIA

As stated in Chapter II, each policy option is assessed using five evaluation criteria. These criteria are compliance with standards, effectiveness, implementation, institutional acceptability, and time. Table 12 summarizes the assessment of Option II against these criteria.

Table 12. Evaluation Criteria Matrix for Option II

Option	Compliance with Standards	Effectiveness	Implementation	Institutional Acceptability	Time
II	Partially compliant	Medium	Moderately difficult	Medium	Minor investment

1. Compliance with Standards

Option II is partially compliant with the NIPP and the NIPP risk management framework. This option complies with the NIPP recommendation to inventory interdependencies during the "Identify Assets, Systems, and Networks" step of the framework. Using Option II the FPS security inspector would identify 10 common interdependencies that may exist for the federal facility being assessed and document the capabilities provided to the facility by the interdependency, links within the facility and with other facilities, and the consequence cost to the tenants in terms of interdependency failure or replacement.

The interdependency data would then be assessed in compliance with the NIPP recommendation that interdependencies should be analyzed using expert judgment or modeling and simulation during the "Assess Risks" step of the risk management framework (DHS, 2006, pp. 12, 31–32, 37; DHS, 2009, pp. 9, 17, 21, 29–32, 35–37). The FPS security inspector would use expert judgment in assessing the security impact of interdependencies within the current FPS Building Security Assessment Program and FSR-Manager frameworks.

Option II is partially compliant with the NIPP because it does not address interdependency networks. The NIPP directs Sector-Specific Agencies to consider relevant cross-sector interdependencies when developing Sector-Specific Plans (DHS, 2006, p. 12; DHS, 2009, pp. 9, 17, 21). Modifying only the FPS Building Security Assessment Program process does not expand the interdependency assessment beyond the facility being assessed. While Option II expands the FPS Building Security Assessment Program by including 10 common interdependencies, the assessment perspective is still primarily focused on one facility.

2. Effectiveness

Option II is assessed as resulting in a medium level of risk reduction. This option will improve the security of one federal facility because interdependencies for that particular building will be factored into the assessments. In order to be assessed as providing a high level of risk reduction, this option would have to incorporate the assessment of multiple federal facilities and their associated interdependencies. The current FPS Building Security Assessment Program and the FSR-Manager would have to be significantly revised. Both methodologies were designed for the assessment of only one facility.

3. Implementation

Implementation of Option II is assessed as being moderately difficult because it will require the revision of only one policy and methodology. This option takes advantage of using the current FPS Building Security Assessment Program and FSR-Manager framework. Rather than recommending a complete revision of the methodology, Option II incorporates NIPP-compliant interdependency identification and analysis into the current process. A critical element of implementation will be additional training for the FPS security inspectors in the field. They will need to learn how to identify the 10 common interdependencies suggested in this option, how to analyze those interdependencies within the current FPS security assessment process, and then how to make appropriate countermeasure recommendations to mitigate the risks that have been identified.

4. Institutional Acceptability

The acceptability rating for Option II is assessed as medium. Option II is expected to be readily accepted by FPS security managers but not readily accepted by the security inspectors who conduct the assessments. FPS security managers are expected to have a better understanding of the NIPP and the NIPP risk management framework. Therefore, they may be more inclined to understand and accept recommendations to update the FPS Building Security Assessment Program to include the identification and analysis of interdependencies.

FPS security inspectors are not educated in or required to understand the NIPP and the NIPP risk management framework. They are almost exclusively focused on the tactical-level Building Security Assessment for each facility to which they are assigned. Therefore, like many significant policy changes, FPS security inspectors are expected to be reluctant to add more steps and additional analysis to an already extensive and comprehensive assessment process. The key to increasing institutional acceptability will be an effective training program.

5. Time

Option II is assessed as requiring a minor time investment. Overall development and implementation are expected to take less than two years. The current FSR-Manager software will not have to be modified to accommodate the recommendations in this option. Modifying the FPS Building Security Assessment Program will require approximately six months for incorporating these recommendations and publishing it as an official directive. Approximately six months will be required for the 11 regional Law Enforcement and Security Program Managers to be trained in the new methodology and for these managers to train the FPS security inspectors in their respective regions.

D. OVERALL ASSESSMENT

Option II would provide FPS with an acceptable and moderately difficult methodology to incorporate interdependency identification and analysis. Use of the NIPP's expert judgment method makes Option II an acceptable alternative because it involves a simple analysis of interdependencies without the aid of sophisticated software modeling and simulation tools. While the outcome provides less detail than a more sophisticated modeling and simulation approach may provide, Option II is much more practical from the implementation, institutional acceptability, and time perspectives (DHS, 2006, p. 37; DHS, 2009, pp. 4, 17, 35).

However, Option II's reliance on expert judgment may lead to inconsistent risk calculations and assessments. Each FPS security inspector may assess the 10 common interdependencies differently and recommend different countermeasures.

IV. OPTION III: MODIFY THE FACILITY SECURITY LEVEL DETERMINATIONS FOR FEDERAL FACILITIES: AN INTERAGENCY SECURITY COMMITTEE STANDARD

A. INTRODUCTION TO OPTION III

Option III was developed because the current *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard* recommends that FPS security inspectors consider interdependencies when calculating the Facility Security Level (ISC, 2008, p. 13). Therefore, it is reasonable to present an option that modifies this Standard to better address interdependency vulnerabilities and risks. Chapter II of this thesis provides a detailed explanation and assessment of the current Facility Security Level calculation. The assessment concluded that this calculation does not adequately address interdependencies and Option III was developed to address these inadequacies. A summary of the assessment from Chapter II is included below as an introduction to this chapter.

The first inadequacy of the current Facility Security Level calculation is that the risks associated with interdependencies are not quantified and equally weighted with the five primary factors in the calculation. Instead, interdependencies are relegated to a subordinate, non-weighted factor in the calculation under the "Intangible Factors" section. Interdependencies are simply suggested as one of many conditions that may be considered in addition to the five primary factors. Therefore, the FPS security inspector either does not include interdependency analysis in the calculation or interdependencies are analyzed amongst other non-related factors in this section.

The second inadequacy is the calculation relies on expert judgment on the part of FPS security inspectors. The Facility Security Level calculation instructions incorrectly assume that FPS security inspectors can apply expert judgment for identifying interdependencies, including their impact on security in the "Intangible Factors," and appropriately determine if the Facility Security Level should be increased a maximum of one level due to risks associated with interdependencies. FPS security inspectors receive no education or training in identifying and analyzing interdependencies. Therefore, it is

unlikely that FPS security inspectors will consider interdependencies in the "Intangible Factors" and the risks associated with interdependency vulnerabilities may not be mitigated. Additionally, if the FPS security inspector does consider interdependencies, there is no standard methodology to provide a consistent and repeatable manner in which to inventory and assess the interdependencies.

B. OVERVIEW OF THE FACILITY SECURITY LEVEL CALCULATION

A brief overview of the current Facility Security Level calculation is provided in this chapter to enhance the reader's understanding of the recommendations included in Option III.

A Facility Security Level is a numerical categorization that is used to determine the appropriate security countermeasures that should be implemented for an individual federal facility (ISC, 2008, pp. 1–3). The final Facility Security Level is based on a scale of I through V. The calculation is based on five equally-weighted security factors: mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. Each factor is assigned a score of one through four based on specific criteria presented in the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard*. The scores assigned to each factor are added to produce a preliminary Facility Security Level (ISC, 2008, pp. 5–6).

Interdependency consideration is included as one of several elements of a sixth, non-weighted security factor, called an "Intangible Factor." The FPS security inspector may use expert judgment and analysis to increase the Facility Security Level a maximum of one level due to interdependencies (ISC, 2008, pp. 5, 13). Table 13 provides an overview of the five factors and how the current Facility Security Level is calculated.

Table 13. Current ISC Facility Security Level Determination Matrix (From Interagency Security Committee, 2008, p. 6)

Factor	Points				Score
	1	2	3	4	
Mission Criticality	LOW	MEDIUM	HIGH	VERY HIGH	
Symbolism	LOW	MEDIUM	HIGH	VERY HIGH	
Facility Population	< 100	101–250	251–750	> 750	
Facility Size	< 10,000 sq. ft.	10,001–100,000 sq. ft.	100,001–250,000 sq. ft.	> 250,000 sq. ft.	
Threat to Tenant Agencies	LOW	MEDIUM	HIGH	VERY HIGH	
					Sum of above
Facility Security Level	**I** 5–7 Points	**II** 8–12 Points	**III** 13–17 Points	**IV** 18–20 Points	Preliminary FSL
Intangible Adjustment	Justification				+ / - 1 FSL
					Final FSL

C. OVERVIEW OF OPTION III

Option III recommends modifying the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard* to include interdependencies when calculating the security level of each federal facility. Rather than being an optional consideration, interdependencies would be the sixth factor of the Facility Security Level calculation and be equally weighted with mission criticality, symbolism, facility population, facility size, and threat to tenant agencies (ISC, 2008, pp. 4–13). A value, points, and criteria matrix, matching those in the current standard, is presented in

order to equally weight interdependencies with the other five factors. This approach may increase the Facility Security Level for buildings that have critical interdependencies and thus require more security countermeasures to protect the facility.

D. DETAILS OF OPTION III

As previously stated, Option III utilizes the same calculation and process steps used in the current *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard*. The proposed option adds the identification and analysis of interdependencies into the calculation. The recommended process steps are explained in the following paragraphs and the modified scoring tables and matrices are included in the explanation of each step. The six steps recommended in Option III are:

- Step 1: Analyze Six Primary Factors
- Step 2: Determine the Overall Value and Points for all Primary Factors
- Step 3: Utilize a Modified Facility Security Level Calculation Matrix
- Step 4: Utilize a Modified Rating Scale to Determine the Preliminary Facility Security Level
- Step 5: Determine Changes in the Preliminary Facility Security Level based on Intangible Factors
- Step 6: Determine the Final Facility Security Level

1. Step 1: Analyze Six Primary Factors

Option III begins with using the existing *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard* to analyze the primary factors of mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. The proposed option recommends using the 10 common interdependencies that were used in Option II (see Table 14) to inventory interdependencies. The FPS security inspector would determine which of the 10 interdependencies exist and then document the capabilities provided to the facility by the interdependencies, interdependency links within the facility and with other facilities, and the consequence cost to the tenants in terms of

interdependency failure or replacement (Lewis, 2006, p. 110). This data would be used in Step 2 of Option III to determine the overall value and points that should be assigned to the "Interdependencies" factor.

The first reason for this step is to clearly define the interdependencies that should be identified and assessed within the context of the Facility Security Level calculation. The current Facility Security Level calculation does not provide clear guidance to the FPS security inspector about which interdependencies to assess. Therefore, using the 10 common interdependencies would provide clear and consistent direction to the security inspector. The second reason is to reduce, as reasonably as possible, the calculation-specific judgment that must be made on the part of the FPS security inspectors. This facilitates consistency in applying the calculation to different facilities across the country. The third reason is to provide a level of consistency between the recommendations made in Options II and III. This is an aspect that will be important for the recommendations made in Option IV, which suggests a hybrid approach using Options II and III.

Table 14. Common Interdependencies for Federal Facilities

Interdependency	Definition
Electrical Power	Primary and backup electrical power sources
Natural Gas Supply	Primary natural gas supply
Water Supply	Primary water supply
Waste Water Disposal	Primary wastewater disposal system
Communications	Voice services provided from or utilized by federal tenant agencies. These include terrestrial, satellite, and wireless transmission systems (DHS, 2009)
Information Technology	Hardware, software, and IT systems provided or utilized by federal tenant agencies. This includes all classified and unclassified Internet connections provided or utilized by federal tenant agencies (DHS, 2009)
Postal Service	Small- and medium-size packages delivered and retrieved by the U.S. Postal Service (DHS, 2009)
Shipping Services	Small- and medium-size packages delivered and retrieved by the commercial courier services (DHS, 2009)
Organizational Connections	Sharing of information, intelligence, products or services within and between organizational elements
Human and Social Factors	Human and social behaviors that exist within the facility and between facilities and should be considered from a security perspective

2. Step 2: Determine the Overall Value and Points for all Primary Factors

Step 2 begins with using the current scoring tables included in the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard.* This step would now include an interdependency scoring table to accurately determine the appropriate points that should be assigned to the additional "Interdependencies" factor. Table 15 shows the recommended value, points, criteria, and examples that can be as scoring criteria. This table is modeled after the current scoring criteria for the mission

criticality, symbolism, facility population, facility size, and threat to tenant agencies factors. Therefore, the "Interdependency" factor can be assessed in the same manner as the five current factors.

Table 15. Recommended Interdependency Scoring Table for the Facility Security Level Calculation

Value	Points	Criteria	Examples
Very High	**4**	Interdependencies support a facility that must remain operational at all times to support National Essential Functions or Essential Functions of the federal government	White House
		Interdependencies support communications centers for National Essential Functions or Essential Functions of the federal government	White House Communications Agency Facilities
		Interdependencies support Continuity of Government or Continuity of Operations for National Essential Functions or Essential Functions of the federal government	FEMA Emergency Operations Center
		Interdependencies support facilities that provide one-of-a-kind or few-of-a-kind services or products for National Essential Functions or Essential Functions of the federal government	Centers for Disease Control and Prevention
		Redundancies in one or more critical infrastructure support element are required to maintain mission performance	Emergency operations centers
High	**3**	Interdependencies support a facility that must remain operational at all times to support Essential Functions of the federal government	National headquarters for federal agencies
		Interdependencies support communications centers for Essential Functions of the federal government	Federal law enforcement communications centers
		Interdependencies support Continuity of Government or Continuity of Operations for Essential Functions of the federal government	COOP sites for national headquarters elements
		Interdependencies support facilities that provide one-of-a-kind or few-of-a-kind services or products for Essential Functions of the federal government	Judicial facilities

Value	Points	Criteria	Examples
		Redundancies in one or more critical infrastructure support element are required to maintain mission performance	Passport production facilities
Medium	**2**	Interdependencies support a facility that provides regional or state-wide functions of the government	General Services Administration regional office
		Redundancies in one or more critical infrastructure support element would enhance mission continuity	Social Security Administration district offices
Low	**1**	Interdependencies support a facility that provides local functions of the government	Local administrative offices
		Redundancies in one or more critical infrastructure support element are not required to maintain mission performance	Local storage facilities

3 Step 3: Utilize a Modified Facility Security Level Calculation Matrix

Option III maintains the same basic Facility Security Level calculation matrix and equal weighting of all the current factors. FPS security inspectors would use the current process and scoring matrices for the factors of mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. Option III recommends adding the "Interdependencies" factor as a sixth equally-weighted factor. Rating interdependencies is directly related to the mission criticality element of the Facility Security Level calculation. The more critical the mission is within a particular federal facility, the more critical it is to assess the risks associated with interdependencies. For example, a facility that houses a federal agency engaged in National Essential Functions should require a detailed identification and analysis of interdependencies to ensure those interdependencies are protected in order to maintain mission accomplishment. Such protective measures may be identified and implemented by increasing the Facility Security Level. Therefore, the "Interdependencies" factor of the calculation is assessed immediately after "Mission Criticality."

Table 16 shows the proposed Facility Security Level Calculation Matrix.

Table 16. Proposed Facility Security Level Calculation Matrix (After Interagency Security Committee, 2008, p. 6)

	Points				Score
Factor	1	2	3	4	
Mission Criticality	LOW	MEDIUM	HIGH	VERY HIGH	
Interdependencies	LOW	MEDIUM	HIGH	VERY HIGH	
Symbolism	LOW	MEDIUM	HIGH	VERY HIGH	
Facility Population	<100	101-250	251-750	>750	
Facility Size	< 10,000 sq. ft.	10,001-100,000 sq. ft.	100,001-250,000 sq. ft.	>250,000 sq. ft.	
Threat to Tenant Agencies	LOW	MEDIUM	HIGH	VERY HIGH	
					Sum of above
Facility Security Level	**I** 6-7 Points	**II** 8-12 Points	**III** 13-17 Points	**IV** 18-24 Points	Preliminary FSL
Intangible Adjustment	Justification				+/-1 FSL
					Final FSL

4. Step 4: Utilize a Modified Rating Scale to Determine the Preliminary Facility Security Level

Option III includes a minor modification to the scale for assigning a preliminary security level of I through IV. This option maintains the use of the sum of the six factor

scores to determine the preliminary security level. However, the upper and lower numbers of the rating scale are increased to 24 and six, respectively, to account for adding a sixth factor to the calculation.

Maintaining the current point scale without significant modification, while still adequately addressing interdependencies, is a very important matter. Facility Security Levels for approximately 9000 federal facilities under the purview of FPS were all re-calculated during fiscal year 2009 using the current calculation. Adjusting the Facility Security Level scale would require re-calculating all the Facility Security Levels once again and could potentially lead to significant changes for many facilities. Table 17 shows the modified rating scale with associated Facility Security Levels.

Table 17. Modified Rating Scale for Determining Facility Security Levels (After Interagency Security Committee, 2008, p. 6)

Facility Security Level	I	II	III	IV
Sum of Factor Ratings	6-7 Points	8-12 Points	13-17 Points	18-24 Points

5. Step 5: Determine Changes in the Preliminary Facility Security Level Based on Intangible Factors

Option III maintains the current "Intangible Factors" element to be used at the discretion of the FPS security inspector. Certain factors may necessitate the adjustment of the Facility Security Level up or down one level. For example, an FPS security inspector may determine there is an interdependency associated with the facility being assessed that is not listed among the 10 common interdependencies. The security inspector may still use the "Intangible Factors" element to adjust the final Facility Security Level. Additionally, the "Intangible Factors" element may still be used for conditions related to the facility that may not be accounted for in the six primary elements (ISC, 2008, pp. 13–14).

6. Step 6: Determine the Final Facility Security Level

The final step of Option III is to determine the final Facility Security Level by adding the scores from the six equally-weighted elements and adjusting the level one point higher or lower according to the "Intangible Factors" assessment (ISC, 2008, p. 6).

The output of this entire calculation would be a Facility Security Level that now accounts for 10 common interdependencies and is adjusted to increase security countermeasures to protect the facility from threats and vulnerabilities associated with interdependencies.

E. ASSESSMENT AGAINST EVALUATION CRITERIA

As stated in the introductory chapter, each policy option is assessed using five evaluation criteria. These criteria are compliance with standards, effectiveness, implementation, institutional acceptability, and time. Table 18 summarizes the assessment of Option III against these criteria. A brief review of the criteria is provided after the table to facilitate understanding.

Table 18. Evaluation Criteria Matrix for Option III

Option	Compliance with Standards	Effectiveness	Implementation	Institutional Acceptability	Time
III	Partially compliant	Medium	Moderately difficult	Low	Minor investment

1. Compliance with Standards

Option III is partially compliant with the NIPP and the NIPP risk management framework. This option complies with the NIPP recommendation to inventory interdependencies during the "Identify Assets, Systems, and Networks" step of the risk management framework. Using Option II the FPS security inspector would identify 10 common interdependencies that may exist for the federal facility being assessed and

document the capabilities provided to the facility by the interdependency, links within the facility and with other facilities, and the consequence cost to the tenants in terms of interdependency failure or replacement.

The interdependency data would then be assessed in compliance with the NIPP recommendation that interdependencies should be analyzed using expert judgment or modeling and simulation during the "Assess Risks" step of the risk management framework (DHS, 2006, pp. 12, 31–32, 37; DHS, 2009, pp. 9, 17, 21, 29–32, 35–37). The FPS security inspector would use expert judgment in assessing the interdependency in order to determine the overall value and points that should be assigned to the "Interdependencies" factor.

Option III is partially compliant with the NIPP because it does not address interdependency networks. The NIPP directs Sector-Specific Agencies to consider relevant cross-sector interdependencies when developing Sector-Specific Plans (DHS, 2006, p. 12; DHS, 2009, pp. 9, 17, 21). Modifying only the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard* does not expand the interdependency assessment beyond the facility being assessed.

Option III is also partially compliant because it does not produce security countermeasure recommendations that are specific to each of the 10 common interdependencies in accordance with steps four and five of the NIPP risk management framework (Prioritize and Implement Protective Programs) (DHS, 2006, pp. 12, 31–32, 37; DHS, 2009, pp. 9, 17, 21, 29–32, 35–37). The only outcome of Option III is the Facility Security Level. While this level is used to select security countermeasures in accordance with Interagency Security Committee standards, those countermeasures are not necessarily directed to mitigate potential risks associated with interdependencies. Additionally, the Facility Security Level is primarily used as a categorization tool, not a complete risk analysis too. Therefore, modifying only the Facility Security Level calculation falls short of properly analyzing the interdependencies.

2. Effectiveness

Option III is assessed as resulting in a medium level of risk reduction. This option will improve the security of one federal facility because interdependencies for that particular

building will be factored into the assessments. In order to be assessed as providing a high level of risk reduction, this option would have to incorporate the assessment of multiple federal facilities and their associated interdependencies. The *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard* was designed for the assessment of only one facility or one cluster of federal facilities (called a federal center or campus) and would have to be significantly revised to include interdependencies across multiple federal facilities (ISC, 2008, p. 14).

3. Implementation

Implementation of Option III is assessed as being moderately difficult because it will require the revision of only one standard. This option takes advantage of using the current *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard* framework. Rather than recommending a complete revision of the Facility Security Level calculation, Option III incorporates NIPP-compliant interdependency identification into the current process. A critical element of implementation will be additional training for the FPS security inspectors in the field. They will need to learn how to identify the 10 common interdependencies suggested in this option and how to analyze those interdependencies within the revised Facility Security Level calculation included in this chapter.

4. Institutional Acceptability

The acceptability rating for Option III is assessed as low. Option III is not expected to be readily accepted by FPS security managers and inspectors for two reasons. One, the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard* was published in February 2008, just one year prior to the writing of this thesis. FPS managers are not expected to be willing to modify the *Standard* so soon after it has been published.

Second, the Facility Security Levels for all 9000 federal facilities under the purview of FPS were re-calculated during fiscal year 2009 using the current Standard. FPS is not expected to be willing to re-calculate the Facility Security Levels using a new standard. A

possible resolution for this issue is to incorporate the changes recommended in Option II into the three-year and five-year recurring Building Security Assessment schedule.

5. Time

Option III is assessed as requiring a minor time investment. Overall development and implementation of the recommendations are expected to take less than two years. Modifying the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard* will require approximately six months for incorporating these recommendations and publishing the new Standard. Approximately six months will be required for the 11 regional Law Enforcement and Security Program Managers to be trained in the new methodology and for these managers to train the FPS security inspectors in their respective regions.

F. OVERALL ASSESSMENT

Option III would produce a Facility Security Level determination that is adjusted according to the interdependencies associated with the facility. The assumption is that a higher security level would lead to the implementation of additional security measures, thus adequately addressing the potential risks associated with interdependencies. However, this option falls short of accounting for and modeling the network formed by the interdependencies and the potential effects on security across this network.

Option III would provide FPS with an acceptable and moderately difficult methodology to incorporate interdependency identification. This option relies on the use of the expert analysis per the NIPP. It may be an acceptable alternative because it involves a simple analysis of interdependencies without the aid of sophisticated modeling and simulation tools. While the outcome provides less detail than a more sophisticated modeling and simulation approach may provide, Option III is practical from the implementation and time perspectives (DHS, 2006, p. 37; DHS, 2009, pp. 4, 17, 35).

V. OPTION IV: DEVELOP A COMPREHENSIVE REGIONAL SECURITY ASSESSMENT STRATEGY

A. INTRODUCTION TO OPTION IV

Option IV recommends a regional, network-based risk analysis methodology with which FPS can adequately model interdependency networks and provide recommendations to reduce the overall risk to the federal facilities network. This strategy would expand the current building-centric strategy utilized by FPS to include an analysis of the interdependency networks formed by federal facilities and related critical infrastructure. Such a strategy would meet the intent of the NIPP risk management framework, which is to identify interdependencies and then analyze them using modeling and simulation (DHS, 2006, pp. 31–32, 37). The identification phase of the NIPP framework would begin with FPS security inspectors collecting interdependency data and documenting it in the Facility Security Level calculations and security assessments conducted for each federal facility (Option II and III of this thesis). This data would also be used with a modeling tool to show which federal locations and related critical infrastructure should be the priorities for protecting National Essential Functions, Essential Functions of Government, or mission-essential functions for a particular federal agency. The outcome would be a regional, network-based security assessment that would be used to direct the allocation of finite security resources.

B. OVERVIEW OF OPTION IV

Option IV is a four-phase approach to assessing the security of federal facilities. Figure 4 shows the process diagram associated with these four phases and the following paragraphs provide a summary of each phase.

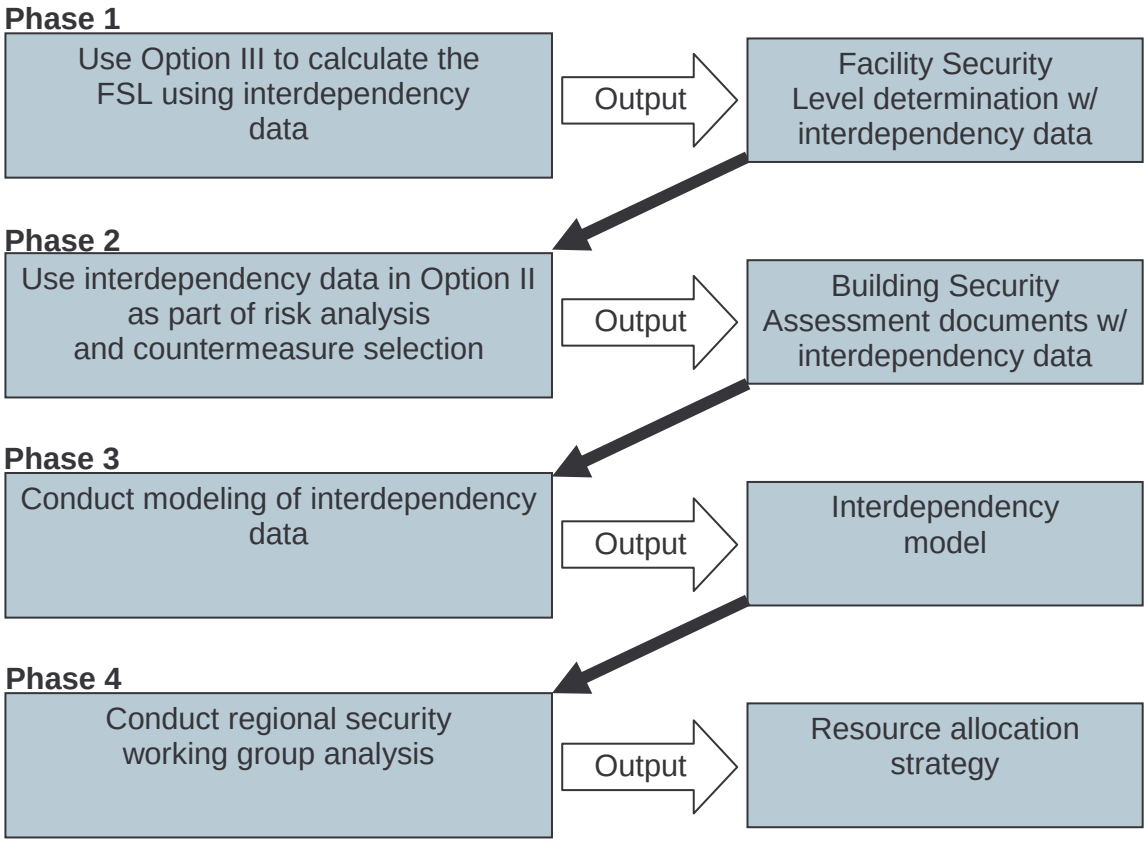

Figure 4. Four Phases of Option IV

Phase 1: Implement Option III of this thesis, which recommends modifying the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard* to include interdependency data collection and analysis in determining the security level for federal facilities. This interdependency data would be used in Phases 2 and 3 of Option IV.

Phase 2: Implement Option II of this thesis, which recommends modifying FPS Directive 07-004, *Building Security Assessment Program,* to include the identification and analysis of interdependency data and making security countermeasure recommends based on this data. These countermeasure recommendations would be tactical-level recommendations based on expert analysis of the 10 common interdependencies recommended in this thesis.

Phase 3: Use a modeling tool, with data collected during Phases 1 and 2 of this option, to model the interdependency network formed by federal facilities. The intended output of the tool would be a broad strategic-level view of federal facility and infrastructure networks so FPS security inspectors and managers can make informed decisions about protecting critical nodes of the network vice individual facilities in isolation.

Phase 4: Regional security assessment working groups analyze strategic- and operational-level interdependency networks and make funding recommendations for protecting critical hubs in the network.

C. KEY ELEMENTS OF OPTION IV

Three elements of Option IV make it a more strategic and comprehensive approach to securing federal facilities than the current FPS methodology. These elements are the regional, network-based approach; the scalability of the strategy; and the building block approach used in execution of this strategy.

1. Regional, Network-Based Approach

The regional, network-based approach expands the security assessment perspective from a single federal facility out to multiple facilities, multiple critical infrastructure sectors, and the networks that connect these facilities and sectors. Utilizing such an approach expands the current facility-centric security assessments out to the operational and strategic levels of FPS and the Government Facilities Sector. This is a key element of Option IV and a major improvement to the FPS security assessment methodology because federal facilities do not exist in isolation and all federal agencies do not operate independent of one another.

2. Scalability

The regional, network-based approach is scalable and can be defined in a manner that is applicable to any organizational level within FPS or in a manner that best suits any particular purpose of a security assessment. For example, the regional, network-based perspective may be defined geographically, organizationally, according to physical connections, or according to human or social factors.

A geographic perspective may be defined by an assessment of a particular city, part of a state, a large region of the country, or even the entire country. Several examples help explain the geographic scalability of Option IV. An FPS supervisor at the operational level may use Option IV to analyze a network of federal facilities within a major city such as Washington, D.C., Los Angeles, or Chicago. An FPS regional director, who has responsibility for multiple states, may use this option to analyze an interdependency network that spans his or her area of responsibility. FPS headquarters personnel may even use this option to conduct a broad, nation-wide analysis of federal facilities.

An organizational perspective also may be used for this regional, network-based security assessment option. For example, a particular federal agency may request that FPS conduct an analysis of how best to protect their multiple federal office locations. Such a perspective could inform how best to allocate that agency's security funding to protect and preserve overall mission accomplishment, determine the critical and mission-essential assets of the agency, and provide data for improving or modifying continuity of operations plans.

Physical connections can be defined as tangible linkages between federal facilities and other critical infrastructure sectors that provide services or products to the federal government. Such connections include electrical power, natural gas and water supplies, information technology assets and networks, and postal and shipping services. Physical connections form the interdependency backbone for federal operations and support the overall business of government in providing services to the public and between agencies.

Human and social perspectives may be used to identify and analyze the human connections that cross organizational and geographic boundaries. Both formal and informal collaboration networks exist within large organizations and between organizations. Oftentimes collaboration networks enable and improve how agencies accomplish their missions, but these networks are not analyzed to determine how critical they are to the functioning of an organization. For example, FPS relies on the assistance of local police departments for law enforcement response to remote locations or federal offices where FPS does not have personnel. Most of this local assistance is provided through informal human and social networks formed without the aid of formal written agreements between

organizations. It may be beneficial from a security perspective to identify these human and social networks, analyze the connections that exist, and determine if critical information hubs exist that may need to be protected.

The scalability of Option IV also facilitates combining all four of these perspectives into the analysis. A security manager or inspector at any FPS organizational level can use data from all perspectives to identify the critical infrastructure elements, regardless of the type, and determine how best to protect the agencies and their critical assets.

3. Building Block Approach

The building block approach used in Option IV is the underpinning of the data collection and analysis of this scalable, network-based strategy. FPS security inspectors collect and document data at the tactical level when they conduct their on-site security assessments and document the interdependency data in the Facility Security Level calculation and Building Security Assessment. This data spans the geographic, organization, physical, and human and social connection elements of the interdependency networks and can be used effectively in which ever analysis perspective is chosen by any level of the FPS organization. In other words, the interdependency data collected at the tactical level for each federal facility builds the data foundation for security analyses that can be performed at the operational and strategic levels of the FPS organization.

D. DETAILS OF OPTION IV

Option IV recommends utilizing Options II and III of this thesis at the tactical level of the FPS security assessment strategy and then adding the use of a modeling tool at the operational level to determine interdependency-related vulnerabilities and the utilization of regional security assessment working groups to recommend appropriate security resource allocation strategies. This option utilizes the bottom-up approach described in the *National Infrastructure Protection Plan* and the building block approach previously described in this chapter.

1. Phase 1

Phase 1 of a regional, network-based security assessment strategy is the first building block of this option. Option III of this thesis, which recommends modifying the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard,* would be used in its entirety. Option III recommends that FPS include interdependencies in the Facility Security Level calculation for each federal facility.

Calculating the Facility Security Level is the first step in the FPS security assessment process and would be an appropriate first building block of Option IV. By implementing Option III as Phase 1 of a regional, network-based security assessment strategy, an FPS security inspector would collect and document data for the 10 common interdependencies listed in Option III. Two outputs from this phase are critical to this option. First, the Facility Security Level would be appropriately calculated with the addition of interdependency data as one of the six equally-weighted factors. This modified calculation may increase the Facility Security Level for federal facilities that have critical interdependencies and thus require more security countermeasures to protect the facility.

The second output would be interdependency data that would be used in the subsequent phases of Option IV. This data would be used in the modified Building Security Assessment (Option II of this thesis), the interdependency modeling, and the regional security assessment working group analysis. As a reminder to the reader, Table 19 shows the data that would be collected during this phase in order to calculate the Facility Security Level using the 10 common interdependencies.

Table 19. Common Interdependencies for Federal Facilities

Interdependency	Definition
Electrical Power	Primary and backup electrical power sources
Natural Gas Supply	Primary natural gas supply
Water Supply	Primary water supply
Waste Water Disposal	Primary wastewater disposal system
Communications	Voice services provided from or utilized by federal tenant agencies. These include terrestrial, satellite, and wireless transmission systems (DHS, 2009)
Information Technology	Hardware, software, and IT systems provided or utilized by federal tenant agencies. This includes all classified and unclassified Internet connections provided or utilized by federal tenant agencies (DHS, 2009)
Postal Service	Small- and medium-size packages delivered and retrieved by the U.S. Postal Service (DHS, 2009)
Shipping Services	Small- and medium-size packages delivered and retrieved by the commercial courier services (DHS, 2009)
Organizational Connections	Sharing of information, intelligence, products or services within and between organizational elements
Human and Social Factors	Human and social behaviors that exist within the facility and between facilities and should be considered from a security perspective

2. Phase 2

Phase 2 would be the second building block of a regional, network-based security assessment strategy. Option II of this thesis, which is a modification of the current Building Security Assessment process, would be used in its entirety. A modified Building Security Assessment would include interdependency identification and analysis for the facility being assessed. The primary outcome of Option II would be recommendations for appropriate security countermeasures that reduce the risks associated with interdependencies. These tactical-level, building-specific countermeasure recommendations would be based on the

expert analysis of the 10 common interdependencies recommended in this thesis, would provide valuable data for the interdependency modeling, and would inform the analysis to be conducted in Phase 4 of this option.

3. Phase 3

Data collected during Phases 1 and 2 of this option and the resultant outputs and outcomes would be used to model the interdependency network formed by federal facilities and other critical infrastructure. This phase would be conducted at the operational level of FPS by Regional Security Assessment Working Groups. The purpose of the working groups would be to serve as the primary oversight and decision-making bodies within an FPS region for risk analysis and security countermeasure funding at the operational level and to influence the allocation of security funding at the strategic level of FPS. The working group would be chaired by the deputy regional director and membership would include the risk management branch chief, the threat management branch chief, the program manager for law enforcement and security programs, and district commanders. Rather than the current FPS process whereby operational-level managers simply review Building Security Assessments, the Regional Security Assessment Working Group would be fully engaged in the risk analysis process, in particular Phases 3 and 4 of this option.

An analysis of existing modeling tools and a recommendation for a specific tool that could be used by FPS for this phase is outside the scope of this thesis. However, a suitable modeling tool that would support a regional, network-based security assessment strategy should have the attributes similar to those used in Model-Based Risk Assessment. A suitable modeling tool would:

- Accept interdependency data from Phases 1 and 2 of this option. This data includes the 10 common interdependencies recommended in this thesis, federal facilities and critical infrastructure as nodes in a network, and interdependency links between the nodes (Lewis, 2006, pp. 110–111);
- Include input data fields for costs associated with the impact of loss (e.g., elimination costs and consequences costs) of each node and link (Lewis, 2006, pp. 110–111);

- Incorporate threat and vulnerability data associated with each node and link (Lewis, 2006, pp. 112–113); and
- Allow the user to determine the acceptable level of risk reduction based on budget allocation and vulnerability reduction across the entire network or for a specific node or link (Lewis, 2006, pp. 119–136, 145–187).

4. Phase 4

Regional Security Assessment Working Groups would utilize the outputs of Phase 3 to analyze strategic- and operational-level interdependency networks and make funding recommendations for protecting critical hubs in the federal network. The intent of the Working Groups' analysis is to protect the National Essential Functions and Essential Functions of Government by identifying the critical federal hubs that support these functions. Their risk analysis and the subsequent security countermeasure recommendations and funding should remain at the strategic and operational levels, and not duplicate the tactical-level, building-specific countermeasure recommendations that are produced by Phase 2 of this option.

The security countermeasure recommendations made by the Regional Security Assessment Working Groups may include funding for and the protection of critical infrastructure elements outside the Government Facilities Sector. The outcome of this option may include security vulnerabilities related to interdependencies that exist in one of the other seventeen critical infrastructure sectors. Therefore, the Working Group would serve as a strategic- and operational-level body that conducts cross-sector collaboration to protect risks associated with these interdependencies.

The Regional Security Assessment Working Groups would also serve as the strategic-level collaborators for federal security funding across multiple federal agencies. Currently this type of collaboration is primarily conducted at the FPS headquarters level (the strategic level) and by the individual FPS security inspectors (the tactical level). While some collaboration occurs at the FPS regional offices (the operational level), a gap still exists wherein funding discussions about the entire federal facilities network do not occur

and thus interdependency security risks are not addressed. The Working Group would formally fill this gap and provide the regional view of the federal facility network and the interdependencies associated with that network.

E. ASSESSMENT AGAINST EVALUATION CRITERIA

As stated in Chapter II, each policy option was assessed using five evaluation criteria. These criteria are compliance with standards, effectiveness, implementation, institutional acceptability, and time. Table 20 summarizes the assessment of Option IV against these criteria.

Table 20. Evaluation Criteria Matrix for Option IV

Option	Compliance with Standards	Effectiveness	Implementation	Institutional Acceptability	Time
IV	Compliant	High	Very difficult	Medium	Major investment

1. Compliance with Standards

Option IV is compliant with the NIPP and the NIPP risk management framework. This option complies with both the NIPP recommendation to inventory interdependencies during the "Identify Assets, Systems, and Networks" step and the recommendation that interdependencies should be analyzed using modeling and simulation during the "Assess Risks" step of the framework (DHS, 2006, pp. 12, 31–32, 37; DHS, 2009, pp. 9, 17, 21, 29–32, 35–37). Ten common interdependencies that may exist for federal facilities would be identified during Phase 1 of this option. The analysis and modeling of interdependencies would occur during Phases 2 through 4 of this option.

2. Effectiveness

Option IV is assessed as resulting in a high level of risk reduction. Security will improve across a network of federal facilities because interdependencies are factored into the assessments. FPS should experience risk reductions at the tactical, operational, and strategic levels of the organization. Tactical, building-specific risks are mitigated during the

assessment portions of Phases 1 and 2 of this option. Operational and strategic risks are mitigated across a broad geographic region during the modeling and risk analysis portions of Phases 3 and 4 of this option.

3. Implementation

Implementation of Option IV is assessed as being very difficult because it will require significant policy revision and training on the part of FPS. Phase 1, which recommends modifying the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard*, was assessed as being moderately difficult to implement in Chapter Four of this thesis. Phase 2, which recommends modifying the Building Security Assessment process to interdependency data collection and analysis, was assessed as being moderately difficult in Chapter Three of this thesis. Adding the modeling of interdependency data and the risk analysis by a Regional Security Assessment Working Group to these moderately difficult phases will make Option IV very difficult to implement.

FPS does not currently utilize any modeling tools so extensive research and testing would be required to select an appropriate tool. New policies and procedures would have to be published to direct and guide the phases recommended in Option IV. Implementation would require extensive training for FPS personnel at all levels, including headquarters, regional, district, and area level personnel. Training in all phases of Option IV would have to be added to the curriculum at the FPS Physical Security Training Program.

4. Institutional Acceptability

The institutional acceptability rating for Option IV is assessed as medium because it is expected to be readily accepted by FPS managers at the headquarters level, but not readily accepted by regional managers and the security inspectors who conduct the assessments.

The FPS headquarters risk management division has acknowledged the importance of including interdependency analysis in the FPS risk management methodology. Several telephone conversations regarding interdependency analysis as it relates to the Government Facilities Sector indicate that FPS headquarters may accept Option IV or a similar recommendation (M. Harvey & P. Kacha, personal communication, October 2008 to

September 2009). However, this high level of acceptance at FPS headquarters must be balanced with the expected low level of initial acceptance at the operational and tactical levels. Incorporating interdependency analysis in the field will require a significant paradigm shift. Regional, district, and area level directors, commanders, and security managers will be transitioning to the new Risk Assessment and Management Program during fiscal year 2010. Implementing Option IV may be viewed as an additional, significant change from FPS headquarters and may not be welcomed. The combination of a high level of expected acceptance at FPS headquarters with an expected low level of acceptance in the field yields a rating of medium for institutional acceptance.

5. Time

Option IV is assessed as requiring a major time investment. Overall development and implementation of Option IV is expected to take more than two years. Phase 1, modifying the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard,* will require approximately one year to incorporate these recommendations and publish a new standard. Phase 2, modifying the FPS Building Security Assessment Program, will require approximately one year to incorporate these recommendations and to publish a new directive. The development and implementation of both phases could run concurrently. Future research will have to determine how long it would take to incorporate Option IV into the new Risk Assessment and Management Program methodology after it is implemented in the field.

Developing and implementing Phases 3 and 4 are expected to take more than two years. An appropriate interdependency modeling tool would have to be researched, tested, and selected. New policies and procedures would have to be published to direct and guide the phases recommended in Option IV. Implementation would require extensive training for FPS personnel at all levels, including headquarters, regional, district, and area level personnel. Training in all phases of Option IV would have to be added to the curriculum at the FPS Physical Security Training Program. All of these steps would require a significant time commitment from FPS as an institution.

F. OVERALL ASSESSMENT

Option IV is assessed as being the most compliant option with regard to the NIPP and the NIPP risk management framework. This option complies with both the NIPP recommendation to inventory interdependencies during the "Identify Assets, Systems, and Networks" step of the framework and the recommendation that interdependencies should be analyzed using modeling and simulation during the "Assess Risks" step of the framework (DHS, 2006, pp. 12, 31–32, 37; DHS, 2009, pp. 9, 17, 21, 29–32, 35–37). Option IV is also expected to result in the highest level of risk reduction when compared to the other options. The trade off for achieving anticipated high levels of NIPP compliance and risk reduction will be very difficult implementation, a medium level of institutional acceptability, and over two years for full implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. COMPARATIVE ANALYSIS, CONCLUSION, AND FUTURE WORK

Chapter VI presents a comparative analysis of the four options presented in the previous chapters and the results of this analysis are reviewed. The preferred option for identifying and assessing the network of interdependencies that exists between federal facilities and other critical infrastructure is presented and defended in the conclusion. Future work related to the implementation of the preferred option is presented at the end of this chapter.

A. COMPARATIVE ANALYSIS AND RESULTS

Chapters II through V each concluded with an assessment of the proposed policy option using the five evaluation criteria: compliance with standards, effectiveness, implementation, institutional acceptability, and time. Each policy option was assessed independently against the evaluation criteria without comparing the options against each other or against the most favorable ratings that a preferred option should receive.

Table 21 shows the results of each assessment compiled into one table for review and analysis. The reader will notice that a fifth option, titled the "Ideal Option," was added to the table. The "Ideal Option" represents the preferred ratings for each of the five evaluation criterion. In other words, the "Ideal Option" answers the question, "What ratings would a hypothetical, most preferred option receive?" The "Ideal Option" was used as a comparison tool to determine which of the four options presented in this thesis should be recommended as the best option.

Table 21. Evaluation Criteria Matrix for All Options

Option	Compliance with Standards	Effectiveness	Implementation	Institutional Acceptability	Time
I	Non-compliant	Low	Simple	High	No investment
II	Partially compliant	Medium	Moderately difficult	Medium	Minor investment
III	Partially compliant	Medium	Moderately difficult	Low	Minor investment
IV	Compliant	High	Very difficult	Medium	Major investment
Ideal Option	Compliant	High	Moderately difficult	High	Minor investment

An analysis of the results shown in Table 21 indicates that none of the four policy options exactly matches the "Ideal Option." Therefore, further analysis was conducted to determine which of the four options received evaluation ratings that most closely match the "Ideal Option." Figure 5 is a graphical representation of the evaluation results and was used to compare each of the four options against the "Ideal Option."

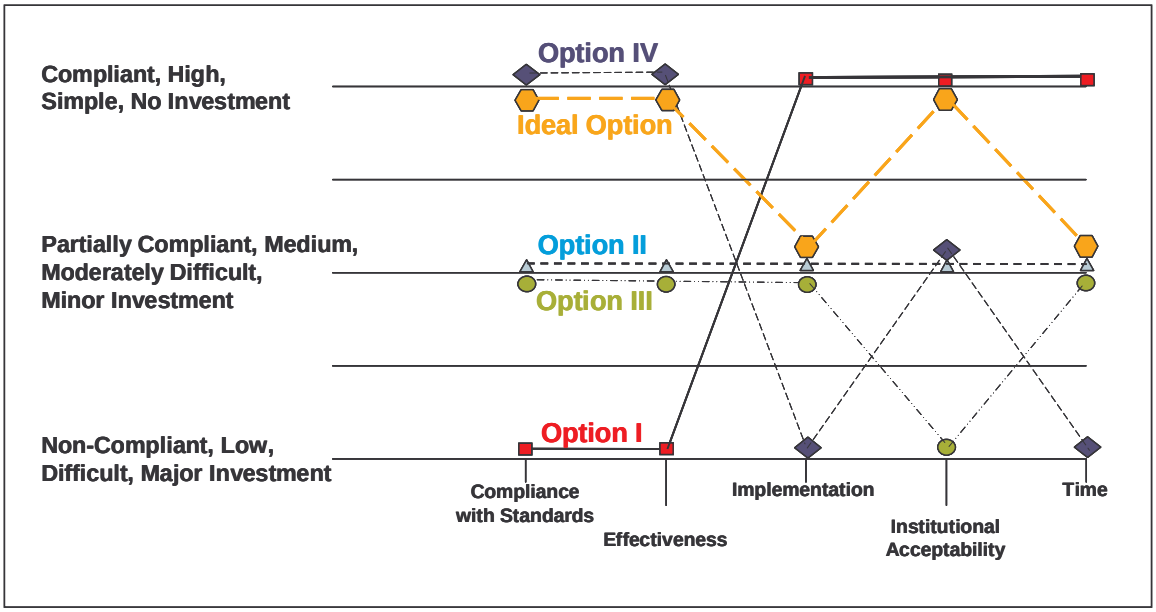

Figure 5. Graphical Representation of All Options

Option I, *Status Quo*, was determined to be the least preferable option. With the exception of the rating for institutional acceptability, the line graph tracks opposite of the "Ideal Option."

Option II, *Revise the FPS Building Security Assessment Program*, was determined to be an acceptable option, although not the preferred option. The line graph tracks exactly in the center of evaluation criteria ratings, making this a middle-of-the-road option. That is, all of the ratings show that Option II would provide a moderate level of improvement to the FPS security assessment program by adding interdependency identification and analysis. However, this option does not expand the program beyond the assessment of a single federal facility in isolation.

Option III, *Revise the Facility Security Level Determination for Federal Facilities: An Interagency Security Committee Standard*, was determined to be unacceptable as a stand-alone option. Like Option II, the line graph tracks in the center of the evaluation criteria rating, with the exception of institutional acceptability which is rated as low. Option III would be considered acceptable either in combination with another option (such as Option IV) or if the institutional acceptability rating can be raised at least to a medium rating.

Option IV, *Develop a Comprehensive Regional Security Assessment Strategy*, was determined to be the preferred option. Figure 6 is the graphical representation of the "Ideal Option" and Option IV without the line graphs of the other three options. One can see from this figure that the line graph for Option IV tracks very closely with the "Ideal Option" line graph.

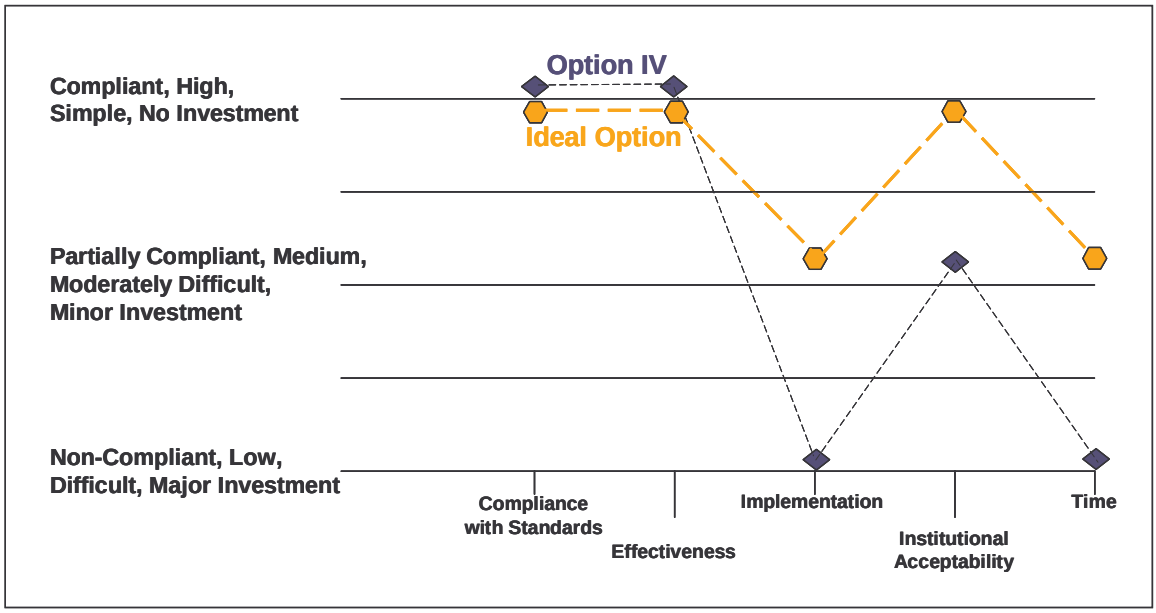

Figure 6. Graphical Representation of Option IV and the Ideal Option

As explained in Chapter II of this thesis, the five evaluation criteria are listed in rank order, ranging from compliance with standards as the most important criteria and time as the least important. Option IV was assessed as having the preferable ratings of "compliant" for compliance with standards and "high" for effectiveness. These are the two most important evaluation criteria, and Option IV matches the "Ideal Option" for both. Option IV was assessed as being difficult to implement, having a moderate level of institutional acceptability, and requiring a major investment of time. All three of these rating are below the "Ideal Option" ratings. However, these ratings are acceptable given the complexity of Option IV. The literature review for this thesis revealed that interdependency identification and analysis is a difficult task. Implementing all four phases of Option IV would be a difficult task for FPS. However, the benefits gained by complying with the NIPP and the NIPP risk management framework, coupled with a highly effective methodology for risk reduction, outweigh the difficulty of implementation. Institutional acceptability can be increased with some specific actions that are outlined later in this chapter. The major investment in time will have to be accepted by FPS as a requirement for implementing such a dramatic change in its risk management methodology.

B. CONCLUSION

The results of the comparative analysis show that FPS should adopt and implement Option IV by developing a comprehensive regional security assessment strategy. Incorporating the identification and analysis of interdependencies between federal facilities and across multiple critical infrastructure sectors presents a strategic value proposition for FPS and other critical infrastructure stakeholders. First, the security of federal facilities can be improved by identifying and mitigating the risks associated with these facilities being interconnected and dependent on other critical infrastructure. Second, the increased collaboration between FPS and other critical infrastructure sectors will assist in achieving the cross-sector coordination that is called for in the NIPP. Third, the continuity of government operations can be improved by protecting interdependencies that support the National Essential Functions and the Essential Functions of Government. Fourth, individual federal agency costs associated with protecting federal facilities may be lowered or costs may be avoided if interdependencies can be identified and protected using a more strategic and regional approach. Additionally, the costs and consequences of a successful terrorist attack may be reduced by identifying interdependencies and increasing their resilience (Kim & Mauborgne, 2006, pp. 23–99).

The interdependency realm presents an opportunity space for FPS (Kim & Mauborgne, 2006, pp. 1–22). Neither FPS nor any other federal agency is currently assessing interdependencies and how the security of federal facilities is impacted positively or negatively by the interdependency network. This opportunity space is available for FPS to address from a protection perspective, but it is also available for terrorists and criminals. Professor Ted Lewis identified that interdependencies may create unnoticed vulnerabilities and seams in the protection of critical infrastructure that can be exploited by terrorists and criminals (Lewis, 2006, pp. 7, 62). FPS should take responsibility for that opportunity space within the Government Facilities Sector and related critical infrastructure sectors before the terrorists and criminals do so. After all, the security of federal facilities is the primary mission of FPS and no other federal agency is charged with this mission.

C. FUTURE WORK

Five issues should be addressed in the future if FPS adopts the recommendations of this thesis. These issues may have a direct impact on the implementation of the recommendations and additional research will be required to properly address all five issues.

The first issue is that FPS should conduct a demonstration project utilizing Option IV of this thesis. One FPS region should collect and analyze interdependency data and determine security resource allocations based on all four phases of the option. This demonstration project would serve to provide qualitative interdependency data from the modeling phase of the option and qualitative data related to the effectiveness of this option in reducing risk.

The second issue is how best to engage multiple stakeholders in a comprehensive regional security assessment strategy. Federal agencies continue to view security of their facilities in the customary "stove pipe" manner because funding is agency-specific. Each agency budgets for and receives security funding for its own facilities through its internal fiscal processes. These processes are not conducive to the cross-agency, cross-sector regional security assessment approach recommended in this thesis. FPS will have to educate its federal stakeholders in this regional-level security assessment process, how to apply the FPS regional recommendations to countermeasure funding, and how to implement those countermeasures from a regional perspective vice the current agency-specific perspective.

FPS will also have to determine how best to engage non-traditional and possible non-federal stakeholders in the regional-level security assessment process. These stakeholders may include representatives from other critical infrastructure sectors that are part of the network of interdependencies. For example, private corporations such as electricity companies may need to be engaged in the regional security assessment process if an interdependency vulnerability related to electrical power is identified by a Regional Security Assessment Working Group.

The third issue is security countermeasure funding. The security countermeasure funding policy should be modified to provide the Regional Security Assessment Working

Groups with flexibility to authorize funding to protect critical federal hubs. The funding policy should also link security countermeasure funding to the annual FPS budgeting cycle for the region so critical hubs will receive regional funding vice building-specific or agency-specific funding.

The fourth issue is change management at the FPS regional level and within the FPS training division. FPS headquarters should develop a structured management model to assist regional staff members with transitioning to the regional security assessment strategy and for forming the Regional Security Assessment Working Groups. FPS training division staff should incorporate all of the recommended strategies and policy updates into the curriculum of the Physical Security Training Program. This staff should also form mobile training teams to educate regional staff members and security inspectors in the updated strategies and policies.

The fifth issue is incorporating interdependency identification and analysis into the Risk Assessment and Management Program (RAMP). During the first two quarters of fiscal year 2010, RAMP and its associated software and databases will replace the current Building Security Assessment process and the FSR-Manager software. The first iteration of RAMP will not include interdependency analysis. FPS should consider the recommendations presented in this thesis and determine if they can be incorporated into future iterations of the RAMP methodology. The new RAMP methodology may be used in Option IV and simply replace the process step that includes the soon-to-be obsolete Building Security Assessment. Alternatively, the research and concepts in this thesis may be used to develop and implement an interdependency module that can be incorporated into RAMP in the near future.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX

Critical infrastructure—Assets that are so vital to the United States that their destruction or degradation would have a debilitating effect on the essential functions of government, national security, the national economy, or public health. Key resources are very similar, but the impact of their destruction or degradation would have a minimal impact (U.S. Congress, 2002, pp. 6, 130). Critical infrastructure and key resources (CI/KR) are used synonymously in this thesis to avoid confusion and because they are closely related.

Consequence—The result of a terrorist attack or other hazard that reflects the level, duration, and nature of the loss resulting from the incident (DHS, 2006, p. 103).

Essential Functions of Government—Government functions that enable federal Executive Branch agencies to provide vital services, exercise civil authority, maintain the safety and well-being of the general populace, and sustain the industrial/economic base in an emergency (ISC, 2008, p. 2).

Federal Facility—Buildings and facilities owned or leased in the United States and occupied by Federal Executive Branch agencies excluding most Department of Defense activities (ISC, 2008, p. 2).

National Essential Functions—Functions of the federal government that are necessary to lead and sustain the nation during catastrophic emergency and must be supported through Continuity of Operations and Continuity of Government programs (ISC, 2008, p. 2).

Risk—A measure of potential harm that encompasses threat, vulnerability, and consequence; the expected magnitude of loss due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss (DHS, 2006, p. 105).

Risk Management Framework—A planning methodology that outlines the process for setting security goals; identifying assets, systems, networks, and functions; assessing risks; prioritizing and implementing protective programs; measuring performance; and taking corrective action. Public and private sector entities often include risk management frameworks in their business continuity plans (DHS, 2005, p. 105).

Sector-Specific Agency—Federal department or agency that is responsible for critical infrastructure protection of a specific sector (DHS, 2006, p. 105).

Sector-Specific Plan—Plan that augments the *National Infrastructure Protection Plan* and provides specific details for protecting a particular critical infrastructure or key resources sector (DHS, 2009, p. 111).

Threat—A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property (DHS, 2009, p. 111).

Vulnerability—A weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary, or disrupted by a natural hazard or technological failure (DHS, 2009, p. 105).

LIST OF REFERENCES

Anderson, C. W., Barker, K., & Haimes, Y. (2008). Assessing and prioritizing critical assets for the United States Army with a modified RFRM methodology. *Journal of Homeland Security and Emergency Management, 5*(1), 1–21.

Applied Research Associates, Inc. (2001). *FSR-manager FPS v2.0 user's guide*. Washington, D.C.: author.

Bardach, E. (2005). *A practical guide for policy analysis: The eightfold path to more effective problem solving*. Washington, D.C.: CQ Press.

Buchanan, M. (2002). *Nexus: Small worlds and the groundbreaking science of networks*. New York: W.W. Norton & Company, Inc.

Chittester, C., & Haimes, Y. (2004). Risks of terrorism to information technology and to critical interdependent infrastructures. *Journal of Homeland Security and Emergency Management, 1*(4).

Federal Protective Service. (2007). *Building security assessment program*. Washington, D.C.: author.

Federal Protective Service. (2008). *Final ISC facility security level implementation strategy*. Washington, D.C.: author.

Federal Protective Service. (2009). *RAMP questions of the week*. Messages posted each week by the Risk Management Division of the Federal Protective Service.

Haimes, Y. Y. (2002, June). Roadmap for modeling risks of terrorism to the homeland. *Journal of Infrastructure Systems*, 35-41.

Haimes. Y. & Horowitz, B. (2004). Adaptive two-player hierarchical holographic modeling game for counterterrorism intelligence analysis. *Journal of Homeland Security and Emergency Management, 1*(3), 1–19.

Haimes, Y. & Horowitz, B. (2004, June). Modeling interdependent infrastructures for sustainable counterterrorism. *Journal of Infrastructure Systems*, 33–42.

Homeland Security Council. (2007). *National strategy for homeland security*. Washington, D.C.: author.

Interagency Security Committee. (2008). *Facility security level determinations for federal facilities—An interagency security committee standard*. Washington, D.C.: author.

Jiang, P. & Haimes, Y. (2004). Risk management for Leontief-based interdependent systems. *Risk Analysis, 24*(5), 1215–1229.

Kim, W.C. & Mauborgne, R. (2006). *Blue ocean strategy: How to create uncontested market space and make the competition irrelevant*. Boston, Massachusetts: Harvard Business School Press.

Kunreuther, H. (2007). *Risk management strategies for dealing with interdependencies.*. Philadelphia, Pennsylvania: Risk Management and Decision Processes Center, Wharton School of the University of Pennsylvania.

Lewis, T. (2006). *Critical infrastructure protection in homeland security: Defending a networked nation*. Hoboken, New Jersey: John Wiley & Sons, Inc.

National Commission on Terrorist Attacks upon the United States. (2004). *The 9/11 Commission report: Final report of the National Commission on Terrorist Attacks upon the United States*. New York: W.W. Norton & Company, Inc.

Office of Homeland Security. (2002). *National strategy for homeland security*. Washington, D.C.: author.

Pink, D. (2005). *A whole new mind.* New York: Riverhead Books.

Sewage and Water Board of New Orleans. (2009). *Report on current and future capital needs 2006.* Retrieved March 14, 2009, from: http://www.swbno.org/

U.S. Congress. (2002). *Public Law 107–296, Homeland Security Act of 2002*. Retrieved October 10, 2008, from http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

U.S. Department of Homeland Security. (2009). *Critical infrastructure and key resources sectors*. Retrieved April 19, 2009, from http://www.dhs.gov/xprevprot/programs/gc_1189168948944.shtm

U.S. Department of Homeland Security. (2007). *Government facilities critical infrastructure and key resources sector-specific plan as input to the national infrastructure protection plan*. Washington, D.C.: author.

U.S. Department of Homeland Security. (2009). *Interim integrated risk management framework*. Washington, D.C.: author.

U.S. Department of Homeland Security. (2006). *National infrastructure protection plan*. Washington, D.C.: author.

U.S. Department of Homeland Security. (2009). *National infrastructure protection plan*. Washington, D.C.: author.

U.S. Department of State. (2008). *Passports*. Retrieved August 22, 2008, from: http://travel.state.gov/passport/passport_1738.html

U.S. Government Accountability Office. (2008). *The Federal Protective Service faces several challenges that hamper its ability to protect federal facilities* (GAO-08-683). Washington, D.C.: author.

U.S. Government Printing Office. (2007). *The Constitution of the United States*. Washington, D.C.: author.

U.S. Immigration and Customs Enforcement. (2007). *Federal Protective Service strategic plan FY08-FY11*. Washington, D.C.: author.

U.S. Immigration and Customs Enforcement. (2007). *National infrastructure protection plan government facilities sector.* Washington, D.C.: author.

U.S. Legal, Inc. (2009). *Legal definitions.* Retrieved April 19, 2009, from: http://definitions.uslegal.com

White House. (2003a). *Homeland security Presidential directive number 7, critical infrastructure identification, prioritization, and protection*. Washington, D.C.: author.

White House. (2003b). *The National strategy for the physical protection of critical infrastructures and key assets*. Washington, D.C.: author.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Susan Burrill
   Federal Protective Service
   Washington, D.C.

4. Mark Harvey
   Federal Protective Service
   Washington, D.C.

5. Gil Russo
   Federal Protective Service
   Grand Prairie, TX

   Melissa Shafford
   Federal Protective Service
   Grand Prairie, TX

6. Randall Briggs
   Federal Protective Service
   Grand Prairie, TX