2018

Does Cybersecurity Law and Emergency Management Provide a Framework for National Electric Grid Protection?

Matthew Ryan Ziska
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Matthew Ziska

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Tim Bagwell, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Mi Young Lee, Committee Member,
Public Policy and Administration Faculty

Dr. Lynn Ann Wilson, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Does Cybersecurity Law and Emergency Management Provide a Framework for National Electric Grid Protection?

by

Matthew Ryan Ziska

MBA, University of Phoenix, 2003

BS, Metropolitan State University of Denver, 2000

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration – Emergency Management

Walden University

January 2018

Abstract

The U.S. government is responsible for protecting the country's energy and technology infrastructure. Critics argue the United States has failed to prepare, protect and respond to incidents involving the national electric grid leaving communities vulnerable to prolonged power outages. Protection of investor owned utilities' critical infrastructure is vulnerable to cyber and physical harm from the absence of criminalizing the intrusion of private sector computer networks, the lack of cybersecurity threats in emergency management, and the absence of cyber-intelligent leadership supports this argument. The purpose of this study was to introduce an electric grid protection theoretical concept, while identifying whether cybersecurity law and emergency management, amongst the investor-owned utility community, has an optimized relationship for protecting the national electric grid from harm. Easton's political system input/output model, Sommestad's cybersecurity theory, and Mitroff's crisis management theory provided the theoretical foundations for this study. The study utilized a mixed method research design that incorporated a Likert collection survey and combined quantitative chi-square and qualitative analysis. The key findings identified that cybersecurity law and the use of emergency management in the electric grid protection theory were not optimized to protect the national electric grid from harm. The recommendations of this study included the optimization of the theory elements through educational outreach and amending administrative cybersecurity law to improve the protection of the national electric grid and positively impacting social change by safeguarding the delivery of reliable electric energy to the millions of Americans who depend upon it.

Does Cybersecurity Law and Emergency Management Provide a Framework for National Electric Grid Protection?

by

Matthew Ryan Ziska

MBA, University of Phoenix, 2003

BS, Metropolitan State University of Denver, 2000

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration – Emergency Management

Walden University

January 2018

Dedication

I would like to dedicate this work to the men and women who build America, without you we would not have the infrastructure that protects us, the homes that shelter us, and the comforts that we enjoy in this country.

Acknowledgments

I would like to express my sincere appreciation to the following individuals and organizations that supported this study: Sara and Kiley Ziska for your love, patience, and support to achieve the high expectations and continuous improvement that I place upon myself; Dr. Tim Bagwell, Dr. Mi-Young Lee, and Dr. Lynn Wilson for your mentorship and guidance to complete this project; Dr. Erfan Iberhiem and Jory Maes for providing reviews for study validation; Bill Lawrence, Beth Garrnat, and the Electric Information Sharing and Analysis Center for partnering with me to launch this study and providing it to the utility industry; to the many participants who made this study possible; and finally, to my employer, who showed me the importance of energy production, transmission, and distribution services.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Introduction

In this study, I examined the practical elements of a proposed electric grid protection theory. The theory is a conceptual lens that will advance the discussion and contribute to the public policy body of knowledge that addresses cybersecurity law and emergency management. This study acts as an orientation to the real problems facing the United States' ability to protect the electric network of the critical infrastructure sector from cyber and physical harm. In this study, I focused on the electric industry and two pillars of the proposed theory, being acutely aware that additional research in this area will need to be conducted to have a complete understanding of the proposed theory.

In this study, I was concerned with understanding how cybersecurity law and emergency management influence protection of the national electrical grid. I attempted to understand the gaps in cybersecurity law, particularly in criminal law; how the principles of emergency management are used to respond and recover from events that threaten the national electrical grid; and how both cybersecurity law and emergency management relate providing national electrical grid protective strategy.

Problem Statement

Substantial problems are facing the United States' ability to protect investor-owned utilities' electrical grid critical infrastructure from cyber and physical harm. The absence of criminalizing private sector computer system intrusions, the exclusion of cyber-security threats amid the risks listed in emergency management, and a lack of cyber intelligence at the proper management levels are contributing to the problem of

protecting the United States' investor-owned utilities (Demchak, 2010; Friedman, 2013; Koppel, 2015; Mody, 2001; Walker et al., 2010). It was reported that 132 investor-owned utilities are responsible for providing energy to 220 million Americans across the national electrical grid throughout the United States (Edison Electric Institute, 2016). Electrical grid access has increased since the enactment of the Federal Energy Regulatory Commission's Energy Policy Act following the Enron event in 2002 and the Computer Fraud and Abuse Act (Tomain, 2002). The Energy Policy Act set out to increase fair market competition at the transmission level through decentralization of energy management, while the Computer Fraud and Abuse Act protected government and financial sector computer systems from unauthorized access leaving all other private sector systems vulnerable (Kerr, 2003).

The shift to decentralized energy management coupled with today's Internet network dependency has increased the vulnerability of the electric grid to cyber and physical attack (Brenner, 2013; Kinney, 2005; Mody, 2001; Watts, 2003). These problems may have contributed to the adverse impacts that affected the U.S. government and energy systems abroad; for example, adversaries intruded into the U.S. Department of Energy exfiltrating 104,000 sensitive data records in 2011, 2012, and 2013 and toppled the Ukrainian electric grid in December 2015 causing disruption to 225,000 customers for over 6 hours (Foxbrewster, 2016; Freidman, 2013; Ukrainian Journal, 2016).

National electric grid vulnerability influenced by the identified problems is becoming increasingly significant in public policy. Researchers, such as Demchak, (2010), Mody (2001), and Walker (2010), demonstrated that electrical grid threats had

become an important issue in recent years with an unresolved solution. These researchers suggested further investigation into cyber governance issues, cyber understanding amongst industry leadership, and emergency management assistance in identifying national electric grid protection solutions.

Easton (1957) proposed a political system theory explaining political governance. I used Easton's political system input/out model to express current gaps and possible solutions as a narrative theory and method. Easton's model is shown in Figure 1.

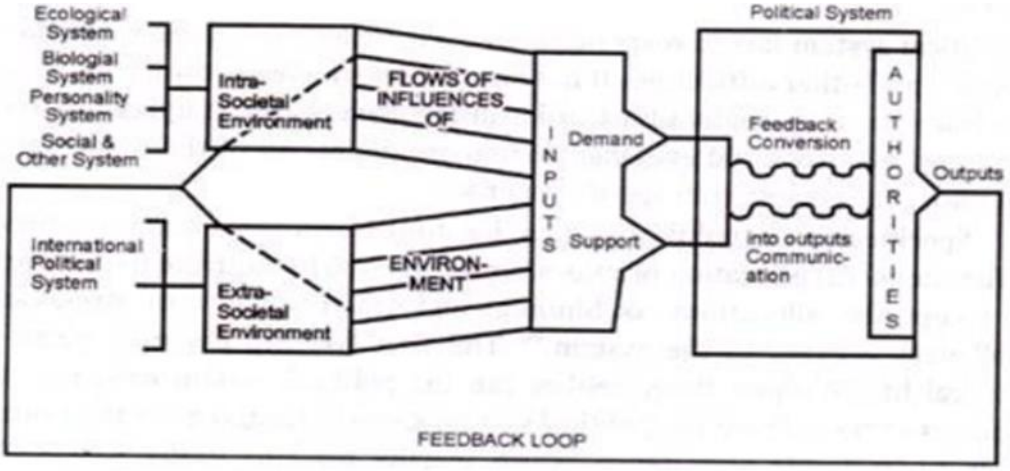

Figure 1. Easton's political system theory input/output model (Pooja, 2016).

Purpose

The goal of this study was to understand the relationship between cybersecurity law and emergency management and the protection of the national electrical grid. I used chi-squared analysis to understand the relationship between cybersecurity law, emergency management, and the national electrical grid.

In this study, I introduced a theoretical framework for national electrical grid protection. The proposed concept relies on cybersecurity law and emergency

management principles being optimized at the national public policy level to be realized as a national electrical grid protection strategy. Cybersecurity law and identified gaps in criminalized computer network intrusions by hackers exposes vulnerabilities that provide access to the national electrical grid critical infrastructure. Emergency management has neglected the integration of its principles into cybersecurity event response and recovery delaying emergency response and recovery efforts to compromised computer network systems owned by investor-owned utilities. Addressing the proposed problems may provide support of the study's proposed electric grid protection theory. Federal government leaders and researchers, such as Brenner (2013), Demchak (2010), Friedman (2013), Mody (2001), and Walker (2010), discussed the elements of the study as independent influencers over electric grid protection, but they have not considered the collective impacts of a single cohesive theory to support national electrical grid protection.

Theoretical Frameworks

The frameworks I used for this study were derived from Crotty's mixed method research conceptualization as presented in Figure 2 (see Creswell, 2011). The epistemological assumption of the framework comes from the blending of the postpositivism and constructivism paradigms. Postpositivism guided the empirical observations in the study, where constructivism guided my proposed electric protection theory through the view of the national electric grid protection phenomenon. Easton (1957), Mitroff (1988), and Sommestad (2012) offered theoretical lenses that underpinned the construction of this study. Easton, a political scientist, proposed a

theoretical system model that I used to form an understanding of input problems within emergency management and cybersecurity law and their relation to national electric grid protection. Mitroff's and Sommestad's academic theories on crisis management and cybersecurity assisted me in developing a broader understanding of emergency management, cybersecurity law, and their gaps as they relate to the protection of the national electric grid in this study.

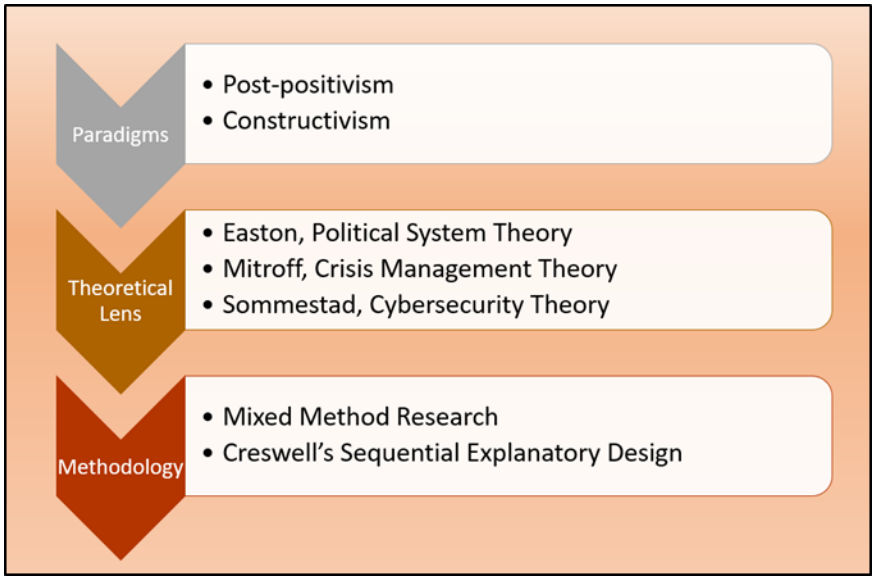

Figure 2. Crotty's mixed methodology theoretical framework.

Operational Definitions

Bulk electric system (BES): Electric generation, transmission lines, interconnections, and associated electrical components necessary to transport high voltage power.

Critical infrastructure (CI): Essential services that support the commerce of the American people (Department of Homeland Security, 2016).

Crisis management (CM): The process strategy that an organization uses to manage a sudden emergency event.

Cybersecurity: The process by which organizations attempt to secure their Internet and Ethernet computer systems from sophisticated adversaries that wish to exploit the organization's information or system (Department of Homeland Security, 2015).

Cybersecurity law: The legal governance that provides procedures for those victimized by computer intrusions can use to take legal action in response to the intrusion.

Cyberspace: Digital virtual space where data are exchanged between a sender and receiver freely.

Emergency management (EM): The process by which an organization prepares for the management of a sudden emergency event by implementing mitigation, preparedness, response, and recovery lifecycle actions.

Energy management system (EMS): The digital infrastructure system that manages the generation and transportation of electricity through the BES.

Hacker: A person, organization, or nation state that uses computer skills to exploit vulnerabilities of computer systems and networks to access to sensitive data, system controls, finances, or other devices.

Industrial control systems (ICS): The general term used to describe computerized systems that control physical engineering and manufacturing processes.

Incident command system (ICS): A standardized management approach to command, control, and coordinate emergency response and recovery actions during a catastrophe.

Investor-owned utility (IOU): A privately-owned energy provider.

Federal Energy Regulatory Commission (FERC): The federal government regulatory organization that governs the generation, distribution, market exchange, and security of the BES.

National electric grid: A series of interconnected networks that deliver electricity from energy providers to consumers across the BES. Its interconnected network consists of generating stations, substations, electrical transmission lines, and electrical distribution lines that deliver energy to individual users.

National Energy Regulatory Corporation (NERC): A federally-sponsored private corporation that conducts research, development, and voluntary regulatory programs for generators and distributors of electricity.

Supervisory Control and Data Acquisition (SCADA): A type of industrial control system that uses a human machine interface to manage the physical engineering process of an industrialized manufacturing system.

Study Assumptions and Limitations

In this study, I assumed the research variables independently supported protection of the national electrical grid. The results of this study could have revealed the research variables to be interdependent possibly impacting the use of Easton's model.

The examination of leadership intelligence was not included in this inquiry. A research study examining leadership knowledge and its relationship to national electric grid protection may be considered in the future. Finally, I did not reflect inclusively all government, public, or private research projects that are investigating additional legal, regulatory, and cyber intelligence use cases to improve the security of the U.S. electric systems in this study.

Significance

The results of this study closed accumulated gaps in the cybersecurity law and national electrical grid security literature with guidance on developing a multivariable conceptual model that may assist the energy industry in securing the national electric grid from cyber and physical harm. As I pointed out in the Problem Statement section of this chapter, the factors presented exist as elements of a conceptual national electric grid protection model that previous studies had not considered as a cohesive framework. If this inquiry is found to support elements of the proposed theoretical model, the research contribution could provide criminal protection against computing system attacks and improve management of events that cause cyber and physical harm to the national electric grid.

National electrical grid protection and providing reliable energy are public policy matters. Electrical power supports individuals, families, economy, health care, transportation, government, and commerce. The inability to protect the national electric grid from harm could cause severe impacts to a population’s ability to function.

Executing this research study to examine these elements created an opportunity for me to improve overall electric EM.

Research Questions

Protecting the national electric grid is a complex problem. I developed the research questions in this inquiry to be rooted in both the postpositivism and constructivism worldviews. In this study, I used Creswell's mixed method approach to blend these worldviews and distinguish justified belief from opinion. The research questions addressed both the quantitative "*top down"* and qualitative "*bottom up"* inquiry approach to determine solutions to protecting the national electric grid (see Creswell, 2008). The research questions were constructed from both worldviews to quantitatively support or reject the research hypotheses and qualitatively explain the observable phenomena.

Easton's (1957) political system input/output model mechanizes the demands (inputs) of a problem to derive solutions, processes, or consequential outputs. With the electric grid protection theory, I considered the demands (cybersecurity law, EM, and national electrical grid) supported by the theoretical stances of cybersecurity and CM. Therefore, the following inputs of the research questions and outputs of the hypotheses were constructed to guide this study:

RQ1: To what extent is there a relationship between EM and the protection of the national electrical grid?

$H_0$1: EM principles focus on physical events and not cybersecurity events, leaving the national electrical grid vulnerable to threats.

RQ2: To what extent is there a relationship between cybersecurity law and the protection of the national electrical grid?

$H_0$2: Cybersecurity law does not provide a legal means to protect the national electrical grid.

RQ3: Does cybersecurity law and EM support a framework to protect the national electrical grid?

$H_0$3: Cybersecurity law and EM currently does not provide a framework to protect the national electrical grid.

Summary

This chapter contained the introduction and background of the study that introduced the electric grid protection theory and its elements. The electric grid protection theory elements were introduced as cybersecurity law, emergency management, and the national electric grid. The study's research introduced the concept that if the study elements have an optimized relationship they may align to provide a protective framework for the national electric grid. Following the introduction, the study's theoretical frameworks were described, and technical operating nomenclature defined. Easton (1957), Mitroff (1988), and Sommestad (2012) offered the theoretical underpinnings for the construction of this study. An overview was provided of the mixed method research design, significance, and introduced the study's research questions.

Chapter 2: Literature Review

Introduction

Protection of investor owned utilities' critical infrastructure is vulnerable to cyber and physical harm from the absence of criminalizing the intrusion of private sector computer networks, the lack of integration of cyber threats into emergency management, and the absence of cyber knowledge at proper management levels. The goal of the study was to understand the relationship between cybersecurity law, emergency management, and the national electric grid to determine if the relationship supports a framework to protect the national electric grid. The literature review provides the context for this study. The chapter contains eleven sections that define the specific themes and elements contributing to the current state of cybersecurity law, emergency management, the national electric grid, and the electric grid protection theory.

The first section defines the bulk electric system, the second section introduces the electric utility industrial control system call the supervisory control and data accusation system, and the third section explains the decentralization of the transmission market. The fourth and fifth sections review public policy relating to the electric grid and cyber governance. The sixth and seventh sections focus on cyber intelligence and attacks on electrical utility systems. The remaining sections describe the principles of emergency management, the electric grid protection theory, and crisis management theory.

Literature Search Strategy

Bulk Electric System (BES)

The modern bulk electrical grid is an energy transportation system built by private utility providers over a century ago (Kinney, 2005). The electric grid is made up of a series of industrial control systems that power generation facilities, transformers, substations, and transmission lines that distribute electrical energy to end users. The power grid is revered as a critical infrastructure that assures reliability with minimal possibility of failure in the United States (Bompard, 2009; Friedman, 2013; Kinney, 2005; Ten, 2010). The electric grid system depends on industrial control systems that regulate electricity load, the balance of load voltages, and balance of frequency to ensure the bulk electrical network is not overloaded or underloaded before the system fails (Bompard, 2009, p. 6; Ginter, 2016).

Independent utility providers developed a series of interconnections to stabilize load balance and share excess generated electricity to improve energy reliability (Bompard, 2009; Kinney, 2005). Centralized utility providers operated the electric grid controlling energy availability, security, and market price (Brenner, 2013; Kinney, 2005). In 1996, the federal government's authority, the FERC, moved to decentralize the control of the electric grid from its centralized structure to ensure competitive market prices and fair consumer costs (Kinney, 2005; Koppel, 2015).

Supervisory Control and Data Acquisition (SCADA) Industrial Control System

Industrial control systems refer to a group of automated physical processes that are responsible for the manufacturing and transportation of energy, chemicals, and petroleum products. Energy production relies on a specific industrial control system called a SCADA system. SCADA systems govern computerized mechanical processes that allow a human control operator to ensure the physical process is safe and reliable (Ginter, 2016).

SCADA systems are an operations technology that is vulnerable to cyber-related attacks. These technologies rely on information technology to protect them from cyber-based attacks (Ginter, 2016). The compromise of SCADA systems by an unauthorized intruder could have grave consequences since it is possible that system controls could be turned over to the intruder creating unsafe conditions and inducing power loss through the shutdown of physical processes (Ginter, 2016; Ten, 2010).

The cybersecurity of SCADA systems has conflicting priorities, and this conflict arises from the integration of information technology with operations technology. Information technology security is fixed in data protection, where operations technology is focused on deterring unauthorized operations from internal or external threats (Ginter, 2016). The information technology and operation technology security discord deters emphasis on life safety being the number one protection priority separating it from the EM processes (Ginter, 2016).

Decentralization of Electric Transmission

The FERC's decentralization of the electric market exposed the electric grid to vulnerability by increasing its cyber network accessibility to multiple utility providers while diminishing leadership decision-making management processes (Tomain, 2002; Brenner, 2013; Koppel, 2015; Watts, 2003). Decentralization of controlled energy markets increased reliability upon the Internet-dependent industrial control systems to operate the entire electric power system from generation to wholesale market trading to consumer distribution (Brenner, 2013; Ginter, 2016; Watts, 2003). The increased reliance on Internet-dependent industrial control systems to manage all aspects of energy management (generation, transmission, distribution, and trade) unlocked the door to increased cyber vulnerability (Ginter, 2016; Watts, 2003).

The federal government placed energy governance responsibility on the FERC. FERC, in turn, created a research and development organization called the NERC to identify energy utility best practices, establish regulations governing reliability, and protect critical electric infrastructure (Watts, 2003). After the September 11, 2001 terrorist attacks, protecting the energy sector was given priority. NERC instituted an Electricity Information Sharing and Analysis Center (EISAC) to assist with electric sector security, counter-terrorism, policy making, and communication between the utility industry and the federal government (Watts, 2003).

Electricity Grid Public Policy and Cyber Space Governance Issues

As previously stated, the bulk electrical network is vulnerable to cyber and physical attacks. In this fast-paced technological world where the electric grid is managed

by the Internet-dependent industrial control systems, such as EM systems, the cyberspace needs strict regulations. In 2015, the U.S. government instituted several public policies to protect the energy infrastructure from cyber and physical attacks. The policies enacted included Fixing America's Surface Transportation Act, Senate Bill S.2012, Physical Security Reliability Standard, Critical Electric Infrastructure Security, Strategic Transformer Reserve, Energy Policy Modernization Act of 2015, Cybersecurity Threats, and Enhanced Grid Security (Parfomak, 2016). These policies had one thing in common, they all addressed the need for enhanced cyber and physical security from energy providers but fell short on how to protect the electric grid from physical attack and cyberspace intrusions. The regulations do not require the cyberspace to be regulated and do not propose measures on how to accomplish cyber governing; in fact, the cyberspace is not regulated spurring debate over legal authority, good governance, increased utility regulation, and the instruments to do so (Demchak, 2010; Mody, 2001). This gap in cyberspace governance enhances the threat of a cyber-attack on the electric grid.

Cybersecurity Regulation and Computer Fraud and Abuse Act

Strict regulation imposed by the FERC authorities increases with each event (cyber, environmental, reliability, etc.) that occurs. Regulations require organizations to improve protective measures, which usually involves costly investments to show regulatory compliance. Although, energy companies are required to adhere to and make substantial investments for regulatory compliance, they are excluded from financial relief during federally-declared disasters. The federal government claims energy is a critical infrastructure, requiring costly compliance to ensure energy reliability and customer

affordability with no financial support for investor-owned utilities or privately-held organizations to recover from a disaster (Stafford Act, 2016). Adversaries of the electric grid may be aware of this lack of federal government support and may look to exploit this gap as a means of resource exhaustion.

The Internet network and the digital cyberspace is not well regulated by an administrative authority (Determan, 2013; Kerr, 2003; Wu, 2013). Lack of regulation stems from poorly defined cybercrime bills that do not specifically address *authorized* and *unauthorized* access (Determan, 2013; Kerr, 2003; Wu, 2013). These terms are referenced in the Computer Fraud and Abuse Act and specifically relate to breach of user contracts leading to civil penalties and not criminal penalties (Determan, 2013; Kerr, 2003; Wu, 2013). The Computer Fraud and Abuse Act was enacted to protect government and financial institutions' "protected computer" systems from misuse by external or internal computer users (Determan, 2013; Kerr, 2003; Wu, 2013). In 2008, the Computer Fraud and Abuse Act was amended to include criminal prosecution of persons who exploit protected computer systems (U.S. Congress, 2017). The amendment recognized illegal activity, such as larceny, and allows for criminal prosecution of those unlawful activities under those specific criminal laws (U.S. Congress, 2017). The bill falls short and does not make the act of unauthorized computer access a criminal action for privately-held computer systems or networks. An Internet network that lacks specific criminal regulation and does not protect computer systems outside government or financial institutions consequentially allow reprehensible actors to intrude with little

negative consequence. The Computer Fraud and Abuse Act was criticized by Wu (2013) describing it as the act as the worst law in technology.

Cyber Intelligent Leadership

In 2008, Senator McConnell raised cybersecurity concerns at the Annual Threat Assessment telling congressional leaders that U.S. commerce was not well protected or prepared to manage a cyber-attack and raising questions about how the government would interact with the private sector to improve the nation's cybersecurity (Sayers, 2008). Sayers (2008) and Koppel (2015) both questioned the ability of current government and private sector executive leadership's ability to provide useful guidance on cybersecurity strategy noting a fundamental lack of computer network security knowledge. Congressional party leaders in Washington acknowledged an immediate need for professional development from both public and private sector leaders who have a depth of cyber knowledge that will improve the national cyber resiliency strategy (Sayers, 2008).

Electric Industry Attacks

The U.S. Department of Energy experienced a cyber intrusion that exfiltrated 104,000 data records in 2011, 2012, and 2013 (Friedman, 2013). In 2015, the Ukrainian electric grid was infected with malware that disrupted electric service to 225,000 customers for over 6 hours (Foxbrewster, 2016; Ukrainian Journal, 2016). The Ukrainian attack is a prime example of grid vulnerability resulting in a cyber-attack that caused physical damages to electrical components through compromised SCADA system that allowed attackers to send commands to ping breakers (Ginter, 2016; Koppel, 2015;

Salmeron et al., 2003; Ten et al., 2010). Pinging is a term used in the utility industry where a command is provided through the SCADA systems to physical system components that signal the equipment to open (turn off) or close (turn on) the flow of electric current. Electrical grid adversaries could develop software algorithms that intrude the power grid's industrial control systems (SCADA), sending out commands to electrical components causing the physical mechanism to fail (Ginter, 2016; Koppel, 2015; Salmeron et al., 2003; Ten et al., 2010).

Cyber algorithms designed by Ten et al. (2010) and Salmeron (2003) have the capability to manipulate SCADA systems that trick human operators by identifying high load electrical imbalances signaling the system to shed load causing the power grid to crash or blackout. The purposes of Ten et al. and Salmeron's studies were to attack the electric grid from the perspective of a terrorist organization with minimal resources to identify cyber vulnerabilities. The fact these studies have been conducted implies that terrorist or adversarial organizations already possess the capability to cause significant cyber and physical damage to the electric grid with few financial or material resources.

Electric Grid Attack Results

The primary concern with a cyber or physical attack on the electrical grid is power loss. The loss of power resulting from an attack can have consequences to the life safety of utility employees and the surrounding population (Ginter, 2016). A life safety event could be the immediate upset of a generation facility or short-term power outages to special populations and additional critical infrastructure. The loss of power for just 1

minute could upset industrial operations causing immediately dangerous to life and health conditions for employees and longer-term consequences to commerce.

Cyber-attacks to the BES have real physical consequences that threaten civility in large population centers. The loss of energy for prolonged periods could create situations of civil unrest, threaten lifesaving operations at hospitals, create extreme seasonal weather environments affecting elderly populations, and cause financial harm to the economy.

Emergency Management (EM)

The U.S. EMS was modeled from the first nationally declared disaster that occurred in Portsmouth, New Hampshire in 1802 (Fugate, 2011). The Portsmouth, New Hampshire disaster was a fire that devastated the port city and threatened commerce in the new nation (Fugate, 2011). In 1802, Congress provided financial disaster relief that assisted the people of New Hampshire to rebuild and incorporate an insurance company to help with asset protection (Fugate, 2011). This disaster relief model of providing financial assistance to victims of a nationally-declared catastrophe has not changed in nearly two centuries.

Today's contemporary EMS evolved to incorporate a physical management structure known as the Incident Command System that organizes actions and communications to one authority (Canton, 2011). The Incident Command System was developed by the Wildland Fire Departments in California in the mid-1970s to manage mass resources and firefighting operations. The Incident Command System was nationally adopted as the National Incident Management System following the terrorist

attacks on September 11, 2001. The cumbersomeness of the Incident Command Systems has excluded cybersecurity resources (cyber-based organizations or functions) from situational awareness, planning, response, and recovery from new events (Walker, et. al., 2010). The exclusion of Cybersecurity-based resources from traditional EM may be due to a lack of cyber knowledge, tools, response priorities, and responsiveness to a cyber-based emergency (Friedman, 2013; Ginter, 2016, Koppel, 2015; Walker et al., 2010). This gap in EM needs closure to ensure a cyber-attack on the critical electric infrastructure can be effectively mitigated.

Electrical Grid Protection Theory

The electrical grid protection theory considers the authoritative decision-making system that optimizes the phenomenon of electrical grid protection based on the pillars of EM, intelligence, and public policy. The three pillars must be in an enhanced state to function accurately in the decision-making system's input/output process.

Easton's (1957) political system theory demarcates the authoritative decision-making processes of society's political system. The political system's demarcations are the inputs from the societal environment that are transformed into consequential outputs that take the form of authoritative decisions or public policy (Easton, 1957). The political system relies on the inputs to work and decision-making outputs consequently which are not unlike other decision-making processes where governance exists.

Crisis Management (CM) and Cybersecurity Theoretical Frameworks

Crisis management theory explains mitigation, preparedness, response, and recovery decisions during and after a catastrophe. The theory uses a Jungian internal and

external risk matrix process and portfolio archetype that determines the consequential probability of risk and severity (Mitroff, 1998). The data derived from the risk model is then used by government or business leaders to derive CM decisions.

SCADA systems are the industrial control mechanisms that govern the physical processes in an industrial manufacturing setting (Ginter, 2016; Sommestad, 2012). Cybersecurity theory is fixed on the premise that protection of data using information technology security approaches produces a secure environment against malware threats for electrical utility industrial control systems (Sommestad, 2012). Sommestad's theory yielded an input/output SCADA cybersecurity risk model that can be used to assess SCADA systems to create security preparedness decisions.

The CM and cybersecurity theoretical frameworks compliment Easton's (1957) political system theory and the proposed electrical grid resilience theory identifying inputs (threats, vulnerabilities, and frequencies) and outputs (preparedness measures) using a system to conceive emergency preparedness policy.

Summary and Conclusions

The literature search strategy introduced the concepts of the BES, SCADA; the decentralization of the electric transmission market; reviewed current cybersecurity law; the concepts of EM principles and crisis management; and explained the electrical protection theory. The literature search identified gaps in cybersecurity law to protect privately owned organizations from hackers, the lack of cyber threat concepts in EM, and lack of cyber knowledge in the management ranks of private organizations. The study closes the gaps identified through the recommended solutions for optimizing

cybersecurity law, EM, and management knowledge in Chapter 5. Further discussion and validation of the identified gaps are found in Chapters 3, 4, and 5.

Chapter 3: Research Method

Introduction

As previously stated, the goal of this study was to understand the relationship between cybersecurity law, emergency management, and the national electric grid to identify if these variables together present a protection strategy against cyber and physical harm to the BES. This chapter examines and defines the study's methodology, sources of data collected, ethical concerns, the study's design, and details the study quantitively and qualitative procedures used and the study's survey tool. The study's methodology was a mixed method sequential explanatory research design introduced by Creswell (2011). The study's participant pool was made up of 132 IOUs. Ethical concerns of the study were addressed by maintaining study participant confidentiality and allowing participants to exit the study at any time. The study's survey was developed and delivered to participants using the software solution SurveyMonkey.

Method of Study

I conducted this study using Creswell's (2011) mixed method sequential explanatory research design as shown in Figure 3. The design blends both the postpositivism and constructivism worldviews allowing for a flexible and thorough method of inquiry. The sequential aspect of the design allowed me to first investigate the empirical tenets of the theoretical lenses of the study by questioning the relationship between cybersecurity law, EM, and the national electric grid. The results derived from the quantitative investigation in the study guided the second qualitative study where I

collected supportive explanation from participants who had experience with cybersecurity law, EM, and the national electric grid.

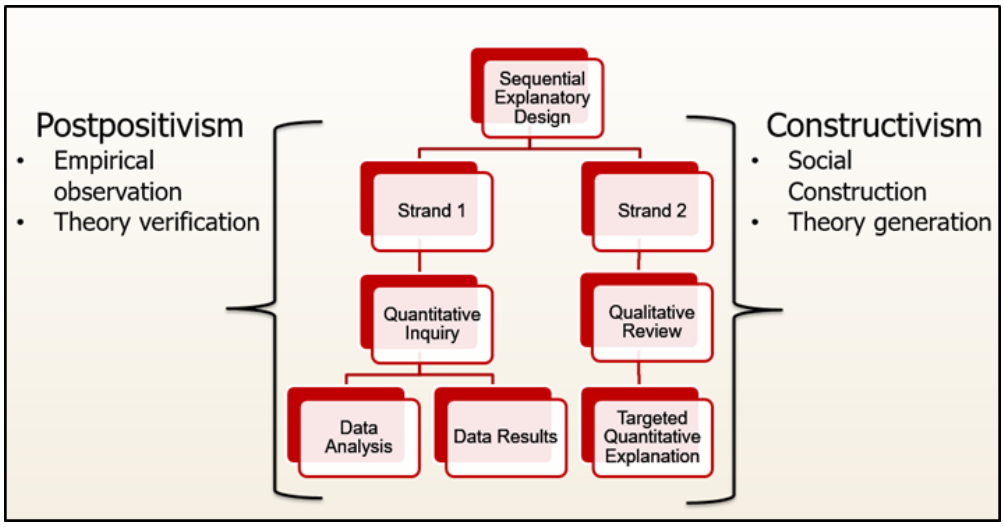

Figure 3. Creswell's sequential explanatory mixed methods research design.

Sources of Data

The data sources I identified and used for this study were collected from 132 IOU companies whose personnel were issued a survey, legal documents, trade association documents, personal interviews, and government documents. The Electric Information Sharing and Analysis Center issued the survey to their utility companies and 118 IOU members completed the survey (see Appendix A). Legal documents and research information from the Colorado Information Sharing and Analysis Center, Federal Legislature, Appellate Courts, Government Accountability Office, and the National Energy Renewable Laboratory was used to gather past and current situational awareness that could potentially support or refute the proposed grid resilience theory. I conducted personal interviews during the second qualitative strand of this study with utility

members from the private sector based on the results in Strand 1 (see Creswell, 2008, pp. 80–81).

Ethical Concerns

The study participants' confidentiality was an ethical concern that I kept at the forefront of my mind throughout the duration of the study. A confidentiality breach may be a perceived risk factor that could cause harm to the study's participants. This ethical concern was considered a low to moderate risk factor, and I addressed it by disabling the online survey Internet Protocol address tracking feature and using informed consent forms during participant interviews. Interview participants had the right to exit the study at any time. The names of study participants were not disclosed in this study. The Walden University research approval number for the study was 06-02-17-0537824.

Study Design

As previously stated, the study design I used was a mixed methodological approach incorporating a sequential explanatory design (see Creswell, 2011). I conducted a quantitative inquiry initially, followed by a qualitative review (see Creswell, 2011). I selected this plan to conduct an empirical investigation to support the proposed conceptual theory with the flexibility to use further investigative techniques to provide further supporting narrative.

I conducted the sequential explanatory design in two research sequences. The first was the quantitative sequence that was underpinned by the postpositivist worldview. This quantitative phase concluded after the results had been finalized. The second sequence was the qualitative inquiry that built upon the quantitative results (see Creswell, 2011).

The qualitative results provided an opportunity for me to explain targeted findings. The qualitative research sequence was underpinned by a constructivist worldview (see Creswell, 2011).

Data Collection Procedures

To collect data for this study, I used Creswell's (2008) gathering procedure for mixed method research. The data collection procedure is visually represented in Figure 4.

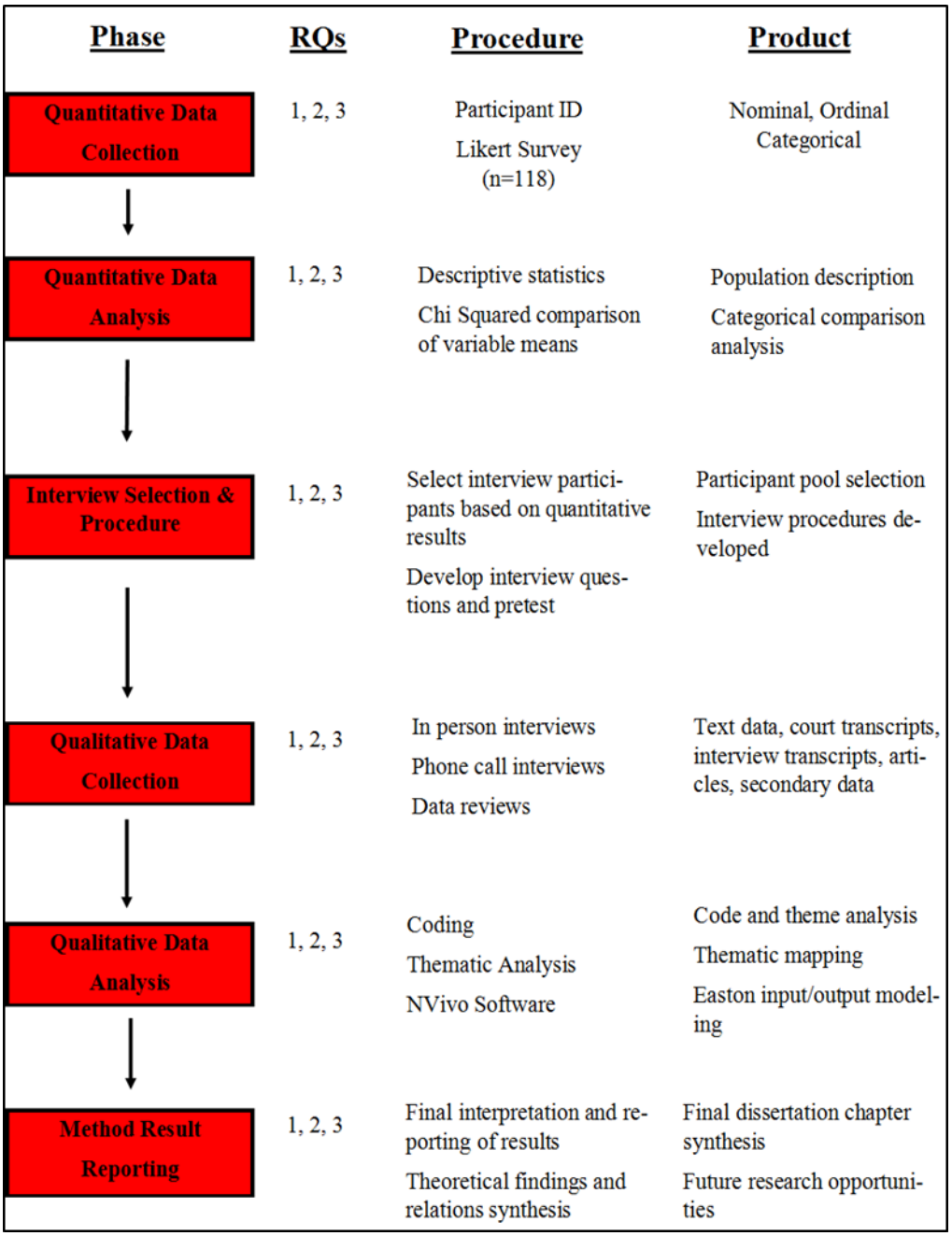

Figure 4. Visual outline of research design procedures.

Quantitative Procedures

The quantitative research procedure is as follows:

1. Quantitative data collection.

a. Develop quantitative research questions using the Survey Monkey instrument

b. Sample population identification

i. Population (*N*) is 132 IOUs

ii. Sample population (*n*) is calculated at 118 using a sample size calculator with a confidence level (CL) of 95% and a CI of +/-3.

iii. Identify research participants within the IOU.

Research participants will be comprised of individuals who occupy the following positions:

- Executive leaders,
- Utility personnel,
- Emergency managers,
- Trade associations, and
- Government agencies.

c. Obtain sample permission(s).

I used the Electricity Information Sharing and Analysis Center to socialize and gain participation in the research study from their members who represented the 118 IOU participants. The organization deployed the participant e-mail letter and study to members from the 118 IOUs.

d. Collect data. I developed a Likert scale survey to survey the sample population. The survey was deployed using the web-based Survey Monkey application.

2. Quantitative data analysis

a. Interpret data and conduct statistical analysis. Nominal and ordinal data were collected. I used descriptive statistics and chi-squared to analyze the data. Descriptive statistics yielded information describing the population. A Pearson chi-squared test of independence was used to examine if there is a relationship between the variables (see Green, 2013).

b. Proceed to qualitative data procedure.

Qualitative Procedures

The qualitative research procedures are as following:

3. Interview selection and procedure.

a. Participant interview selection based on statistical trends identified during the quantitative analysis.

b. I developed interview questions based on quantitative results. Interview questions and protocol were prepared prior to data collection. The interview protocol ensured the participant's confidentiality and explained the purpose and scope of the research project to the participants.

4. Qualitative data collection.

a. I conducted in-person and phone interviews with identified participants. The interviews were transcribed for analysis. Recording devices may be used depending on the participant's permission.

5. Qualitative data analysis.

a. I used the NVivo qualitative analysis application for data coding and thematic determination. The NVivo analysis assisted in mapping themes and developing an Easton input/output model that represents the hypotheses of the study.

6. Method result and reporting.

a. Data results were interpreted, and I determined whether the hypotheses were supported or not supported. The findings were reported and the study completed.

I confirmed the qualitative research validity through the peer review process. Peer review from industry and government organizations supported the legitimacy of the study and ensured it represented the issues accurately.

Survey Tool

I collected quantitative data using a Likert Scale survey specifically developed for this study. Likert Scale surveys are used to measure points of view, arguments, frequency of occurrence, significance, consequence, magnitude, and probability of the populous being studied (Creswell, 2011). The survey was divided into sections to assure research question alignment and variable separation for comparison purposes. A chi-squared statistical analysis was used to investigate the distribution and means of the variables of the study to determine if a relationship existed. I used univariate descriptive statistical analysis to describe the sample population.

The first section of the survey collected data to support the study's first research question: To what extent is there a relationship between EM and the protection of the national electrical grid? Survey Questions 1 through 15 asked questions related to

investigating the "extent of" EM used by the sample population as it related to protection of the national electrical grid.

Section 2 of the survey examined Research Question 2: To what extent is there a relationship between cybersecurity law and the protection of the national electrical grid? Survey Questions 16 through 34 asked questions related to a cybersecurity law called the Computer Fraud and Abuse Act. As previously stated, the Computer Fraud and Abuse Act is the foundational law for providing legal computer system or network intrusion protections to government and financial sectors (U.S Congress, 2017). These questions assessed the sample population's familiarity with and use of the law to support the extent to which cybersecurity law has a relationship to provide protection to the national electrical grid.

The final section of the survey, Questions 35 through 37, examined if: cybersecurity law and EM support a framework to protect the national electrical grid? These questions focused on the sample population's knowledge and application of cybersecurity law and EM to determine if these two independent variables supported a framework to protect the national electrical grid dependent variable. The remaining Survey Questions 38 through 45 collected data that define the sample population by size, type, role, and cybersecurity event experience. The close of the survey provided an option for participants to provide their contact information if they wished to participate in a follow-up interview. The study's survey can be viewed in Appendix A.

I developed the survey using the Internet-based Survey Monkey (www.surveymonkey.com) application. Survey Monkey is an Internet-based, third-party

survey service that has been widely accepted by researchers and universities in today's digital age. Survey Monkey allows the researcher to develop a wide variety of surveys both quantitative and qualitative data, conducts statistical analysis, provides graphical data representations, and can identify common themes. Survey Monkey is a convenient tool that allows study participants to complete the survey with ease and allows researchers to view collected data nearly instantaneously.

Survey Monkey provides solutions to ethical concerns such as confidentiality and anonymity by selecting specific survey design option. Survey Monkey allows the researcher to switch the Internet Protocol option to "No" to ensure participant anonymity and confidentiality. In the survey in this study, I did not track the Internet Protocol of participants to ensure their safety and confidentiality.

Summary

The purpose of the mixed method sequential explanatory study was to gain an understanding of the relationship between cybersecurity law, EM, and the national electric grid. An understanding of these variables determines conclusions of if they support a protective framework for the national electric grid and support the conceptual electric grid protection theory. The study was split into quantitative and qualitative strands. The quantitative strand was performed by issuing a survey to 132 IOUs followed by a qualitative inquiry of participants who volunteered for follow-up interviews. The study's design was selected for its flexibility in using multiple investigative techniques. Study participants identifies were kept confidential and participants could choose at any

time to leave the study at any time. Study results and interpretations are evaluated in Chapter 4 and 5.

Chapter 4: Results

Introduction

In this study, I examined to what extent cybersecurity law and EM provide a framework to protect the national electric grid. Three research questions and hypotheses provided a foundation for this study, where I used Creswell's sequential explanatory mixed methods research approach. The research questions and hypotheses that guided this study were:

RQ1: To what extent is there a relationship between EM and the protection of the national electrical grid?

$H_0$1: EM principles focus on physical events and not cybersecurity events, leaving the national electrical grid vulnerable to threats.

RQ2: To what extent is there a relationship between cybersecurity law and the protection of the national electrical grid?

$H_0$2: Cybersecurity law does not provide a legal means to protect the national electrical grid.

RQ3: Does cybersecurity law and EM support a framework to protect the national electrical grid?

$H_0$3: Cybersecurity law and EM currently does not provide a framework to protect the national electrical grid.

The data I collected to answer the research questions were obtained through the initiation of a survey tool and examination of various government and legal documents.

Participant follow-up interviews were planned to be conducted, but the volunteers who expressed interest had left the study at that point.

This chapter will include the data I gathered to answer the research questions and hypotheses of the study. I will present the findings of the study through the sequential explanatory design using the postpositivist and constructivist theoretical lenses.

Participant Demographics

In this study, I invited individuals representing the utility industry in the United States to participate in the initial research survey through the EISAC on June 15, 2017. A total of 183 individual participants completed the survey. Fifty-two participants (28%) represented municipal utilities, where 131 participants (72%) represented IOUs as shown in Table 1. There were seven executive leaders (3%), eight senior leaders (5%), two director level leaders (1%), 15 midlevel managers (8%), 16 front line managers (9%), and 135 participants (74%) who did not provide a position type response. The general distribution of participants who indicated a position type was 26%. Participants represented the following areas in the utility area: corporate services (53%), operations generation (9%), operations distribution (7%), operations transmission (3%), security services/physical security (3%), continuity services (16%), and EM (9%).

My primary focus in this study was on IOUs. The results from the public utility participants were not analyzed. However, the data collected from the public utility participants may be used in a future study.

The names of the IOUs were not included in the study as a measure to provide participant confidentiality. The results from Survey Questions 1 and 44 provided sufficient evidence to reasonably support that data were collected from the minimum number (118) of IOUs required to complete the study. The participants indicated they represented the following seven regions throughout the United States: West (27%), Central (32%), Texas (6%), Southeast (8%), Florida (5%), Mid-Atlantic (8%), and Northeast (14%).

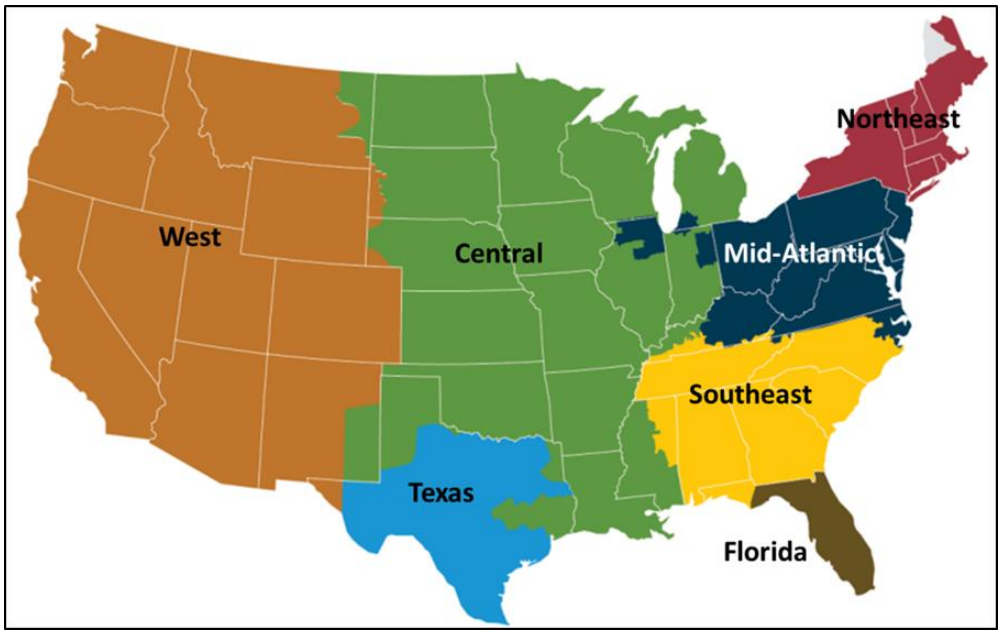

Figure 5. U.S. Energy Information Administration seven region map.

Results Summary

The study was comprised of a survey that asked participants 45 questions to determine whether empirical evidence existed to support the proposed electric grid protection theory. The electric grid protection theory suggests that in an optimized state, the authoritative decision-making system will use EM, intelligence, and public policy as a strategic approach to protect the national electrical grid from cyber and physical threats. The survey I used in the quantitative phase of the study yielded support for the proposed conceptual theory by identifying gaps within the areas of EM, public policy (specifically cybersecurity law), and intelligence in the form of participant knowledge. I also conducted a qualitative review of government-related documents and cybersecurity law case studies following the completion of the quantitative strand of the study. Participant follow-up interviews were not conducted in the qualitative portion of the procedure since most participants declined to participate in the qualitative strand. Four participants who expressed an interest in contributing to follow-up interviews decided to leave the study prior to beginning the qualitative segment. These participants who left the study were concerned about divulging their IOU's confidential proprietary information. It can be inferred that most participants declined the follow-up interviews due to concerns of sharing company proprietary information. I conducted an analysis of participant comments, together with a review of both cybersecurity case law and government regulations, to support the qualitative strand of the study.

I divided the survey study results into categories to represent the three study variables. Questions 2 through 12, 15, and 37 addressed EM; Questions 16 through 24,

35, and 36 addressed cybersecurity law; and Questions 13, 14, and 25 through 34 addressed the national electric grid. The remaining questions collected information about the study participants as I previously summarized at the beginning of this chapter.

I primarily used a statistical analysis technique that included descriptive statistics and chi-squared comparative analysis to examine the data. Descriptive statistics, precisely the mode, was used to show the frequency of the responses and to show the percentage of responses. The chi-square analysis was used to determine significance to support or reject the research hypotheses of the study.

Quantitative Analytical Results

As I stated previously, 131 participants representing 118 IOUs participated in this research study. I administered a survey containing 45 questions to the participants. Participants completed the survey using the Survey Monkey program. The SPSS statistical software was used to perform both descriptive and chi-square statistical analysis on the survey results.

The data I received from the survey used two primary response sets:

- Strongly Disagree, Agree, Disagree, Strongly Agree, and Do Not Know
- Not Confident, Somewhat Confident, Very Confident, and Not Applicable

The response sets were coded in SPSS as shown in Table 2.

Table 2

SPSS Coded Data

Response	Code
Strongly Disagree	1

Disagree	2
Agree	3
Strongly Agree	4
Do Not Know	5 – Missing Value
Not Confident	1
Somewhat Confident	2
Confident	3
Very Confident	4
Not Applicable	5 – Missing Value

I reverse coded Question 17 and used it as a control question to demonstrate the difference between the participants' preceptive knowledge versus their actual knowledge of the Computer Fraud and Abuse Act. Sixty-six percent of participants indicated that they did not know about the Computer Fraud and Abuse Act, while 34% of participants stated that they did know about the Computer Fraud and Abuse Act but failed to answer the control question accurately. The 66% of participants that acknowledged they did not know about the Computer Fraud and Abuse Act and those that answered the control question inaccurately led to Questions 19 through 24 not being included in the statistical analysis to avoid error in the statistical analysis. The question data responses were organized into groups representing the variables of the study.

Descriptive Statistic Analysis Summary

As I previously stated, the study was divided into the three variable categories of EM, cybersecurity law, and the national electric grid. The survey results were not normally distributed, so I transformed the results of the survey into median scores for statistical analysis. The result median scores were used to derive to a more accurate central tendency or distribution of probability.

Participants who indicated "I do not know," "Not applicable," or those who did not provide an answer to a survey question were identified as missing values. The missing values were not included in the statistical analysis. The results for the study variables of EM, cybersecurity, and the national electric grid are summarized in Table 3.

Table 3

Descriptive Statistics

Variable	*N*	Median	*SD*	Skewness	Missing cases
Emergency management	131	3.00	.669	-.646	0
Cybersecurity	116	3.00	.896	-.062	15
National electric grid	91	2.50	1.09	-.001	40

I conducted chi-square analysis to determine if the data results were supportive or nonsupportive of the null hypotheses. Chi-square testing is used to determine the relationship between variables. My chi-Square analysis considered the relationship between EM, cybersecurity law, and the national electric grid to determine if there was quantitative evidence to support the test hypotheses. The results of my chi-square analyses are summarized in Table 4.

Table 4

Chi Square Results

	Statistic	*df*	*p* value	Alpha
Pearson Chi Square	62.3	36	.004	0.05
Phi	.846		.004	0.05
Cramer's V	.346		.004	0.05
Pearson Chi Square	79.7	36	.000	0.05
Phi	.936		.000	0.05
Cramer's V	.382		.000	0.05

Pearson Chi Square	47.6	18	.000	0.05
Phi	.724		.000	0.05
Cramer's V	.418		.000	0.05

The Chi Square analyses for each research question analyzed resulted in a significant value that was less than alpha suggesting a failure to reject the null hypotheses. The Phi and Cramer's Five tests suggest there is an association between the variables. Therefore, there is quantitative support suggesting emergency management principles primarily focus on physical events and not cybersecurity events, cybersecurity law does not provide legal protection for the national electric grid, and EM and cybersecurity law currently does not provide a framework to protect the national electric grid leaving it vulnerable to threats.

Qualitative Analytical Results Summary

The second strand of the study would have examined the study participant's qualitative interview responses to support the study's research questions and further explain the quantitative findings. However, most participants declined to participate in the qualitative phase of the study preventing the ability to conduct follow-up interviews as indicated in the qualitative research procedure presented in Chapter 3. Study participants who had indicated they were interested in participating in follow-up interviews opted to leave the study due to concerns about divulging their investor owned utility's confidential proprietary information. The absence of the follow-up interview data made it difficult to identify thematic trends limiting the use of the NVivo data analysis program.

An examination of the comments that participants provided in the study's survey, Computer Fraud and Abuse Act case law, Incident Command System literature, and government regulation were reviewed to provide further explanation of the study's quantitative results.

Emergency Management (EM), Cybersecurity Law, and the National Electric Grid

The first research question and hypotheses examined the extent of the relationship between EM and the national electric grid. Specifically examining if EM has shifted its focus on physical response to be inclusive of cybersecurity as a measure to reduce the vulnerability to the national electric grid. The study quantitatively demonstrated that EM emphasis is on physical response and not that of cyber event response. A review of Incident Command System publications from Cole (2000), Jain (2003), and Walker (2010) suggested the need to integrate cybersecurity into the Incident Command System without defining an instruction for that integration. Additionally, the Federal Emergency Management Agency's Industrial Control System Cyber Emergency Response Team website did not address integration of cybersecurity into the Incident Command System. The review of literature provided support that emergency management has not been inclusive of cyber related responses.

The second research question placed an emphasis on the relationship between cybersecurity law and the protection of the national electric grid. Specifically examining if cybersecurity law provided a legal strategy to protect the national electric grid. Quantitatively demonstrated cybersecurity law did provide a legal conduit to protect the national electric grid. A review of the Computer Fraud and Abuse Act stated the Act only

applies to the United States government and financial institutions. A case law review indicated that 100% of privately owned businesses who tried to apply the Computer Fraud and Abuse Act to actors who accessed their computer systems without authorization or who exceeded their authorization were overturned in the appellate courts, as described in table 5.

Table 5

Computer Fraud and Abuse Act Case Review

Date	Case Name	Case Number	Judgement	Conviction
9/14/2001	Chance Vs. Avenue A	No. C00-1964C.	Dismissed	No
3/8/2006	International Airport Centers LLC Vs. Citrin	No. 05-1522.	Dismissed	No
3/13/2009	LVRC Holdings LLC Vs. Brekka	No. 07-17116.	Dismissed	No
8/8/2011	College Source Vs. Academy One	No. 09-56528.	Dismissed	No
7/26/2012	WEC Carolina Energy Solutions Vs. Miller & Kelley	No. 11-1201.	Dismissed	No
7/23/2013	Dresser-Rand Vs Jones	Civil Action No. 10-2031.	Dismissed	No

WEC Energy vs. Miller and Kelley demonstrated that an investor owned utility attempting to apply the Computer Fraud and Abuse Act is not protected under the law leaving the organization without a legal protection strategy from individuals who would intrude in their computer system. It further demonstrates current cybersecurity law does

not provide legal protections from those bad actors that would intrude into investor owned utility systems to harm the national electric grid.

The final research question explores if cybersecurity law and EM support a framework to protect the national electric grid. Quantitatively, the study demonstrated that the two variables do not support a framework to protect the national electric grid. The findings can be further supported by examining Presidential Policy Directive 41 and Executive Order on Strengthening Cybersecurity of Federal Networks and Critical Infrastructure (Appendix C; Obama, 2016; Trump, 2017). Presidential Directive 41 stated the federal government would not play a role in supporting a private organization if effected by a cyber event (Obama, 2016). Conversely, the policy expected private organizations to support the government in the event of a cyber incident. President Trump's executive order failed to include response support of the private sector and affirmed that Presidential Directive 41 be followed (see Appendix D). The lack of government support for the private sector leaves the sector vulnerable to cyber related threats extending to the national electric grid. The lack of private industry support by the U.S. government regarding cybersecurity and the absence of cybersecurity integration into the EM principles support the finding that cybersecurity law and EM does not currently provide a strategy to protect the national electric grid from harm.

Electrical Grid Protection Theory

The research study's quantitative and qualitative findings support the research questions hypotheses. The state of the current independent variables, EM, public policy (cybersecurity administrative law), and population knowledgeability was not optimized.

Easton's political system theory applied authoritative decision-making principle, if used in an optimized state, logically dictates that outcomes would result in undesirable decisions. If applied to the protection of the national electrical grid with unoptimized variables, logic dictates the results would not provide protective strategies. However, in an optimized state, the authoritative decision-making principle, logically dictates desirable outcomes.

The electric grid protection theory relies on optimization in the areas of EM and cybersecurity law. Many participants provided neutral responses to the survey questions that were coded as missing value. The result provides support for stating the investor owned utility population may not have the knowledge in EM and cybersecurity law to make optimized decisions regarding protective strategies for the national electric grid. Moreover, the lack of support by the U.S. government for the private sector add to the difficulty of protecting the national electric grid through current cybersecurity law and administrative public policy.

Fortunately, through private and public partnership IOU and the U.S. government have the opportunity to optimize the areas of EM and cybersecurity law to protect the national electric grid from harm.

Conclusion

The findings overall supported the research study hypotheses. The results of both the quantitative and modified qualitative examination demonstrated the IOU population and the study variables are not in an optimized state to provide protective strategies for the national electric grid. The evidence from the study's survey suggests the study

variables are not in an optimized state therefore leading to decisions that may not protect the national electric grid from harm. Qualitative reviews of the literature suggest there are gaps at the federal government's policy level to adequately support the integration of cybersecurity into the Incident Command System and to be inclusive of legal protections for private organizations who experience cyber- related attacks. My full interpretation of the findings of the study will be provided in Chapter 5.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

In this study, I examined elements of a proposed electric grid protection theory. The theory is a concept that explains that optimizing elements could establish a strategic framework for protecting the national electric grid. The theory variables I assessed in this study included EM, cybersecurity law, and their influence on the protection of the national electric grid. The study acted as an academic arrangement to the problem of protecting the U.S. electrical network from harm. In 2015, the Ukraine experienced an electric grid attack while research was being conducted for this study (Ukrainian Journal, 2016). The Ukraine incident caused by a cyber-attack shut down energy production and delivery to 225,000 customers for over 6 hours demonstrating the significance of protecting the power grid (Ukrainian Journal, 2016).

In this study, I identified gaps in cybersecurity law, EM, and IOU employee understanding of the study variables. The gaps identified through the literature review in Chapter 2 and the completion of the study's survey in Chapter 4 included areas concerning criminalizing unauthorized access to computer systems that are not deemed by the federal government as protected systems; principles of EM (i.e., incident command system, event management planning, and cyber-security integration); cybersecurity law; and the national electric grid. In this chapter, I will characterize and attempt to articulate the results of the study.

Interpretation of Findings

There were three problems and three hypotheses that I examined in this study centered around determining the extent that the independent variables had a relationship with the national electric grid and if the independent variables supported a framework to protect the national electric grid from harm. The research hypotheses I developed to forecast the independent variables were not optimized to provide legal protections or a current strategy to protect the national electrical grid from damage. Instead, the research hypotheses integrated with the introduction of the grid protection theory in that the elements of the theory must be optimized so that logical decision outcomes protect the national electric grid from both physical and cyber harm.

EM incorporates the use of life cycle principles and the physical management structure known as the Incident Command System (Canton, 2011). The principles of EM include mitigation, preparedness, response, and recovery (Canton, 2011). Mitigation is the application of measures that will control a threat from causing harmful impacts. The survey questionnaire accounted for relief-related content in Questions 3, 6, 8, 12, and 13. Preparedness includes activities an organization uses to position their resources to respond and recover when a catastrophic event does occur. Preparedness activities include emergency planning, personnel training, education, resource procurement, and conducting emergency exercises (Canton, 2011). The survey preparation related questions were 2, 4, 5, 11, 14, and 15. Response is the deployment of resources and use of emergency procedures to protect life, stabilize an incident, and protect property. Survey Question 5 focused on response management referring to the Incident Command

System. Recovery accounts for the restoration actions (Canton, 2011). Restoration can be acute or long term depending upon the event impacts. Recovery actions could include long term care for displaced individuals and replacement of infrastructure. Survey question 7 addressed recovery from power loss.

The Incident Command System was developed to manage the response to physical catastrophes (Canton, 2011). In today's changing threat environment, cybersecurity has not been integrated into the Incident Command System creating a gap in EM literature (Walker et al., 2010). In Research Question 1 I asked: To what extent is there a relationship between EM and the protection of the national electrical grid?

The questions in Section 1 of the survey were developed to address the first research question. Examining the results, I found that many of the respondents answered the questions with the neutral response, “I do not know.” The responses by most participants in this section suggested the population had a lack understanding of EM and its associated principles and management concepts. Quantitatively, the statistical results and the relationship to the national electric grid indicated a chi square *p*-value less than alpha ($p < 0.05$). The chi square value validated that EM places an emphasis on physical response and not on cybersecurity response leaving the national electric grid vulnerable to threats. The absence of the follow-up interviews with participants to gain insight into their understanding of EM concepts leaves a gap of understanding in my interpretation between EM and the protection of the national electric grid. Additional research studies are necessary to reach this understanding.

Cybersecurity concerns have been raised for more than a decade by experts in the United States. In congressional research briefs, Fischer (2014, 2016) explained that cybersecurity legislation has needed revision and that no overarching framework governing cybersecurity exists. Fifty policies address cybersecurity promoting information sharing and restoration support between the government and private sector (Fischer, 2016). Those 50 policies recently placed by legislative and executive action do not address criminal accountability for bad actors but rather focus on workforce development, information sharing, research and development, data breach prevention, and international policy (Fischer, 2016). Current cybersecurity legislation and executive actions do not mention the Computer Fraud and Abuse Act, which is legislation that was amended in 2008 to make unauthorized access to the computer system in the government or financial sector a criminal offense.

The Computer Fraud and Abuse Act is legislation that criminalizes the intrusion of a computer system from an external or internal individual or organization (U.S. Congress, 2017). The language of the act is clear on who it protects and who could be criminally liable. Legal protection under this act is afforded to government and financial sector computer systems; it is not inclusive of the nonfinancial sector private industry computer systems or networks. The lack of protection for private sector organizations is a gap in the cybersecurity legislation that creates system vulnerabilities exposing the national electric grid to harm. In the second section of the survey, I assessed the participants' attitudes towards the Computer Fraud and Abuse Act and various legislation designed to support response and recovery from a catastrophic failure of the national

electric grid. Questions 16 through 24 targeted the Computer Fraud and Abuse Act. Question 17 was a control question, and if answered in the affirmative the participant's responses were discarded. Sixty-six percent of participants responded that they were not familiar with the Computer Fraud and Abuse Act. Thirty-four percent of participants indicated they were familiar with the act but failed the control question. The responses to Questions 18 through 24 were not included in the statistical analysis, since these responses could have skewed the results.

With the second research question, I examined the extent of cybersecurity law and its relationship to the national electric grid. Specifically, that cybersecurity law does not provide a legal means to protect the national electric grid. $H_0 2$ was quantitatively supported with a chi square result less than alpha ($p < 0.05$). This statistical result was indicative of the responses to the questions regarding the Computer Fraud and Abuse Act. However, the lack of participant interviews could not provide additional insight to ascertain participants' understanding of the Computer Fraud and Abuse Act or related regulation to the national electric grid. My qualitative review of literature further demonstrated the U.S. government's position to be noninclusive of the private sector as it relates to cyber intrusion.

The Computer Fraud and Abuse Act case law review from 2001 to 2013 provided support that cybersecurity law does not protect the private industry. The cases I evaluated involved private organizations attempting to use the law against individuals who gained unauthorized access to their private computer networks or who exceeded their authorization from inside the organization. My review found that in each legal case the

judgment was dismissed, and no convictions were issued. One legal case that I examined was WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012). The case described an IOU organization that filed a criminal law suit against former employees who exceeded their internal computer system authorization for personal gain. The utility group cited the Computer Fraud and Abuse Act and the court dismissed the case.

A framework is the primary underlayment of a system, concept, or structure. In the final research question, I asked: if cybersecurity law and EM support an underlying structure to protect the national electric grid? The statistical chi square analysis resulted in a significant statistical value less than alpha ($p < 0.05$) reinforcing that cybersecurity law and EM currently do not provide a framework that protects the national electrical grid. The quantitative result could be subjective to argument due to the number of cases that were coded as missing value. Furthermore, qualitative interviews of participants were not conducted. Additional quantitative and qualitative research may be necessary to answer this question.

In this study, I observed that EM and cybersecurity law, in an unoptimized state, cannot produce a framework to protect the national electric grid. In the literature review, I identified that EM was focused on physical response and cybersecurity law was not inclusive of the private sector outside of financial institutions.

Electric Grid Protection Theory

I modeled the proposed electric grid protection theory on Easton's political system input/output model in this study. Easton (1957) visualized a conceptual model

that accounted for inputs defined as demands and supports, the decision-making process, and the eventual decisions that govern society. Easton described demand inputs by placing them into two categories: external environmental factors that influence the system and those factors that are generated internally by the system. The internal demands in Easton's explanation describe the motivations of the individuals that advanced the system.

Easton's (1957) model works well when applied to the electric grid protection theory. The inputs in both theories are not dissimilar and rely on environmental demands or inputs. The demands of the electric grid protection theory are defined in three categories: EM, cybersecurity law, and intelligence. Internal motivations consider the actions of individuals to make decisions that govern the generation and delivery of a product to its consumers, in this case, electric energy. I have mentioned for this system to function and produce desirable output decisions, such as those necessary to protect the national electric grid, the three inputs must be in an optimized state. Therefore, it is logical to assert that if the system components are not optimized, the decision-making outputs will produce undesirable results.

In this study, I presented a case that supports the current state of the three categories being in unoptimized positions to be useful in the decision-making process. I hypothesized that the IOU sample population would not be optimized in the EM and cybersecurity law categories. The intelligence category had been defined as knowledge of the categories of individuals in leadership roles but can extended to the awareness of the external societal forces that influence the decision-making process. Most of the sample

population of the study reported they did not have knowledge of the topic of the study by selecting the neutral response in the survey. The observed lack of awareness by participants contributes to the substandard state of the system. An inference can be made from these results that until the three categorical inputs in the system are optimized decisions, that are made to protect the national electrical grid may be undesirable.

Additional research and future research will rely on a measure of the IOU population's understanding of the input areas. This study was a first step in exploring this area of research by introducing a conceptual framework that accounts for an expanded view of elements that may impact protection of the national electric grid.

Limitations of the Study

Methodological assumptions were built into the study. I assumed research participants' answers to the survey questions were honest. I also assumed that my role in the IOU population would instill a level of confidence within the community.

A constraint to the study was realized following the completion of the quantitative investigation. Research participants opted out of the study's qualitative follow-up interviews for concerns of divulging their investor owned utility's proprietary information. The absence of the follow-up interviews data made it difficult to identify thematic trends limiting the use of the Nvivo data analysis program. As such, this study may not represent the population of investor owned utilities. Additional validation of work in this area will be required in the future and will need to include research within the entire electric utility population.

Finally, this study was not inclusive of all the public or private examinations that may have been conducted in this area of interest and needs further investigation.

Implication for Positive Social Change

The national electric grid is a network that energizes the mechanisms for commerce and a fully functional industrialized nation. The loss of energy to commerce could have dire consequences especially if the power failure is prolonged. All sectors of our society's critical infrastructure rely on reliable electric power to operate. Protection of the national electrical grid is a public policy matter that generates decision making that impacts the ability to drive social change.

The study closed gaps in the literature regarding cybersecurity law, EM, and the national electric grid. The electric grid protection theory may assist to advance desirable outcomes in the academic, public, and private industries to better secure the national electric grid from harm. The findings of this study found the elements that make up the theory were not in an optimized state and therefore provides an opportunity to improve social change through the optimization process. Criminalizing unauthorized access into private organizations computer networks may safeguard the national electric grid while extending legal protections not discussed in this study. Improving industry's awareness of EM and its principles will only improve industry's ability to coordinate response, promote protection of life, improve situational stability and protection of property such as the national electric grid.

Recommendations

Protecting the national electric grid from physical or cyber harm is top of mind for lawmakers and the individuals who work in the electric utility industry. The cyber-attack in the Ukraine in December of 2015, made the loss of a life line critical infrastructure a reality around the world. The loss of a critical infrastructure and the industrial control systems that operate them can create dangerous physical conditions that could immediately threaten loss of life, cause severe injury to those who manage the system and those whom the system serves. The study found the pillars of the electric grid protection theory to not be in a state of optimization, concluding that decisions made to protect the national electric grid may be undesirable and may not be effective.

The variables that make up the electric grid protection theory need to be optimized for the decision-making system to work efficiently. Education of the population making up the IOU community will help optimize the system. IOU employees at all levels would benefit from training in the principles of EM and cybersecurity law. The knowledge gained may result in EM leadership levels making effective decisions when developing strategy to secure the national electric grid.

EM principles address the use of the Incident Command System to organize a response to an incident. The Incident Command System was shown to be used for emergencies that result in physical impacts. The Incident Command System would benefit from being updated to be inclusive of a cyber response component to address cyber-related emergencies such as an attack on the national electric grid. Ziska (2017) proposed the inclusion of a cybersecurity section into the general staff of the Incident

Command System (Appendix B). The cybersecurity section would plan the cyber-related response, share information, coordinate with intelligence agencies, and preserve evidence for criminal investigations as shown in Figure 5.

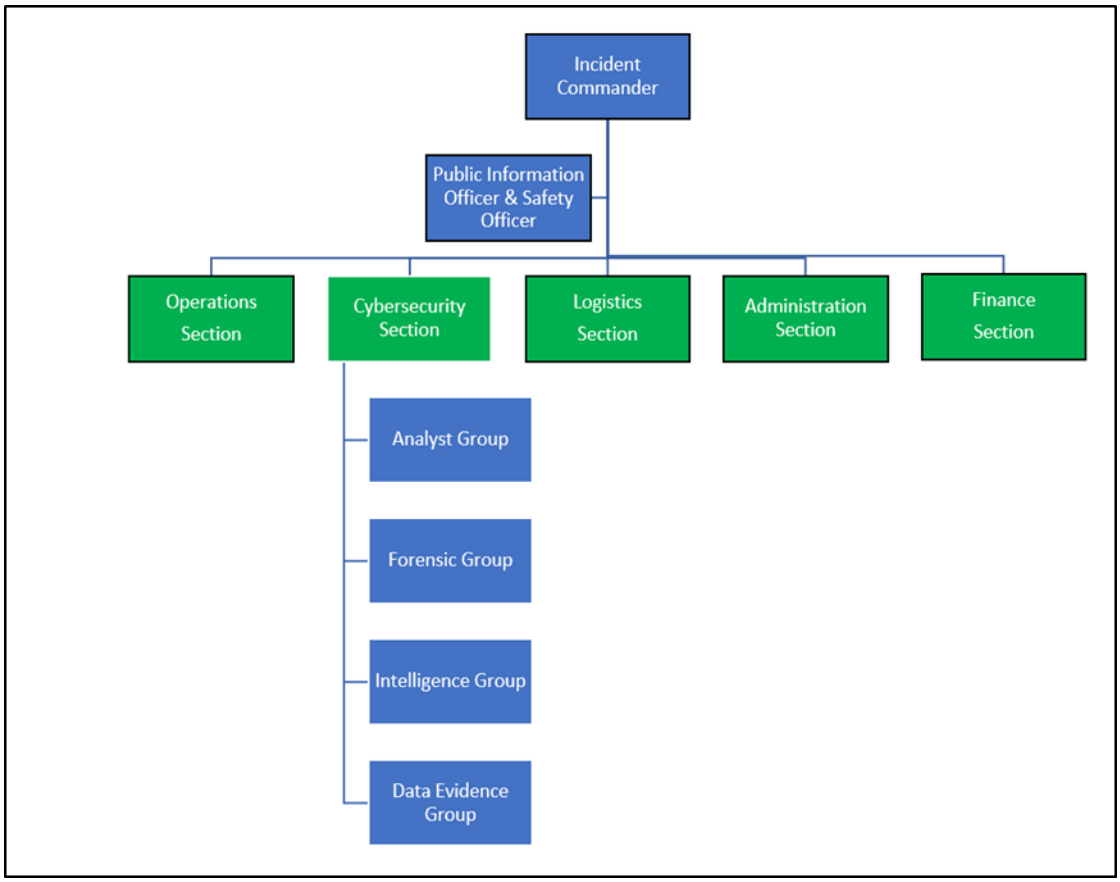

Figure 6. Ziska's cybersecurity integration into the Incident Command System.

Integrating cybersecurity into the Incident Command System provides flexibility to the response by setting up a section that focuses on cyber-related issues while maintaining operational capability to respond to and stabilize physical emergencies or consequences caused by a cyber-attack. Incident Commanders would need to be trained in activating the cybersecurity section. The training for Incident Commanders could

include activation during industrial emergencies or when industrial control system sabotage is suspected.

Finally, cybersecurity criminal law must be defined. The Computer Fraud and Abuse Act address criminal procedures for individuals or organizations who intrude into government and financial sector computer systems or networks. The Computer Fraud and Abuse Act falls short on criminal legal protections of private industry computer systems or networks. The Computer Fraud and Abuse Act needs to be amended to be inclusive of the private sector and the remaining 14 critical infrastructures it does not address. Proposed amended language to the Computer Fraud and Abuse Act can be read in Appendix E. Furthermore, presidential directives, executive orders, or new legislation need to address regulating the cyberspace, dedicating resources to a policing agency, and bringing to justice those individuals who would do harm to our critical infrastructures such as the national electric grid.

Conclusion

Does cybersecurity law and EM provide a framework to protect the national electric grid? The study results expressed the study variables were not optimized as observed by the quantitative responses received by the investor owned utility population and through the qualitative literature review process. The results of the study do not only mean that cybersecurity law and EM do not provide a framework, but rather suggests these variables need to be optimized before they can provide a protective strategy for the national electrical grid.

The survey results reported by the IOU sample population is a baseline that can be used to quantify the population's knowledge of cybersecurity and EM in future studies. The population’s increased awareness in the topic areas will logically produce viable inputs that necessitate the electric grid protection theory's decision-making process to determine actions to improve protection of the national electric grid.

The topic area of securing the U.S. energy delivery system has many factors, and this study focused on two, cybersecurity law and EM. The future of research in this area of interest is vast and the variables plentiful. Future research will need to be inclusive of the entire electric utility population. A study examining EM and cybersecurity law between IOUs and municipal utilities might make for an excellent study to further support the protection of the national electric grid.

References

Aylward, J. (2011). Incident command system at field day. *Qst, 95*, 80-81. Retrieved from https://search-proquest-com.ezp.waldenulibrary.org/docview/868803149?accountid=14872

Bompard, E., Napoli, R., & Xue, F. (2009). Analysis of structural vulnerabilities in power transmission grids. *International Journal of Critical Infrastructure Protection, 2*(1), 5-12. doi:10.1016/j.iicip.2009.02.002

Brenner, J. (2013). Eyes wide shut: The growing threat of cyber attacks on industrial control systems. *Bulletin of the Atomic Scientists, 69*(5). doi:10.1177/0096340213501372

Canton, G. (2011). *Emergency management: Concepts and strategies for effective programs.* City, State: Wiley-Blackwell. Retrieved from VitalBook file.

Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001).

College Source, Inc. v. Academy One, Inc., 653 F.3d 1066 (9th Cir. 2011).

Cornell University Law School. (2016). 16 U.S. Code 8240-1-Critical electric infrastructure security. Retrieved from http://www.law.cornell.edu.

Creswell, J. (2008). *Research design: Qualitative, quantitative, and mixed methods approaches.* Los Angeles, CA: SAGE Publications, Inc.

Creswell, J., Clark, P., & Vicki, L. (2011). *Designing and conducting mixed methods research.* Los Angeles, CA: SAGE Publications, Inc.

Davies, G., Deric, M., & Davies, B. (2005). The incident command system. *Electric Perspectives, 30*(6), 60-64. Retrieved from https://search-proquest-

com.ezp.waldenulibrary.org/docview/217562933?accountid=14872

Demchak, C. (2010). *Conflicting policy presumptions about cybersecurity: Cyber prophets, priests, detectives, and designers, and strategies for a cybered world.* Washington, DC: Atlantic Council.

Department of Homeland Security. (2016b). What is critical infrastructure. Retrieved from https://www.dhs.gov/what-critical-infrastructure

Department of Homeland Security. (2016a). Cybersecurity overview. Retrieved from https://www.dhs.gov/cybersecurity-overview

Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610 (E.D. Pa. 2013).

Easton, D. (1957). An approach to the analysis of political systems. *World Politics, 9*(03), 383-400. Retrieved from http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=7620832&fileId=S0043887100008261

Energy Information Administration. (2012). Electricity. Retrieved from http://www.eia.gov/electricity/data/eia861/.

Federal Energy Regulatory Commission. (2014). Physical security reliability standard. Retrieved from http://www.ferc.gov.

Fischer, E. (2014b). Federal laws relating to cybersecurity: Overview of major issues, current laws, and proposed legislation. Retrieved from https://fas.org/sgp/crs/natsec/R42114.pdf

Fischer, E. (2014a). Cybersecurity issues and challenges: In brief. Retrieved from https://fas.org/sgp/crs/misc/R43831.pdf

Foxbrewster, T. (2016). Ukraine claims hackers caused Christmas power outage. *Forbes Security.* Retrieved from http://www.forbes.com/sites/thomasbrewster/2016/01/04/ukrainepower-out-cyber-attack/#69c0f3225e6f

Frankfort, C., & Nachmias, D. (2007). *Research methods in the social sciences.* Tampa, FL: Worth Publishers.

Friedman, G. H. (2013). *Cybersecurity breach* (DOE Publication No. IG-0900). Washington, DC: U.S. Office of Inspector General.

Fugate, C. (2011). *Evolution of emergency management and communication (FEMA).* Washington, DC: U.S. Senate Committee on Appropriations Subcommittee on Homeland Security.

International Airport Centers, LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

Ginter, A. (2016). *SCADA Security what's broken and how to fix it.* Calgary, Alberta: Abterra Technologies Inc.

Green, S., & Salkind, N. (2013). *Using SPSS for Windows and Macintosh: Analyzing and understanding data* (7th ed.). Upper Saddle River, NJ: Pearson Education.

Jain, S., & McLean, C. (2003, December). Simulation for emergency response: A framework for modeling and simulation for emergency response. *Proceedings of the 35th Conference on Winter Simulation: Driving Innovation,* 1068-1076.

Kinney, R., Crucitti, P., Albert, R., & Latora, V. (2005). Modeling cascading failures in

the North American power grid. *European Physical Journal B – Condensed Matter, 46*(1), 101-107. doi:10.1140/epjb/e2005-00237-9

Koppel, T. (2015). *Lights out* (eBook Version 1). Retrieved from Kindle.com

LVRC Holdings Lcc v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

Mitroff, I., Pauchant, T., & Shrivastava, P. (1988). The structure of man-made organizational crises: Conceptual and empirical issues in the development of a general theory of crisis management. *Technological Forecasting and Social Change, 33*(2), 83-107. doi:10.1016/0040-1625(88)90075-3

Mody, S. (2001). National cyberspace regulation: Unbundling the concept of jurisdiction. Stan. *J. Int'l L., 37*, 365.

Patton, M. (2015). *Qualitative research & evaluation methods: Integrating theory and practice.* Thousand Oaks, CA: SAGE Publications, Inc.

Parfomak, P. (2016). Electric grid physical security: Recent legislation. CRS Insight. Retrieved from https://www.fas.org/sgp/crs/homesec/IN10425.pdf

Sommestad, T. (2012). *A framework and theory for cybersecurity assessments* (Doctoral dissertation, Royal Institute of Technology, Stockholm, Sweden).

Teddlie, C., & Tashakkori, A. (2009). Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences. Thousand Oaks, CA: SAGE Publications, Inc.

Tomain, J. (2002). The past and future of electricity regulation. Environmental Law, vol. 32, No. 2, 2002. Pp. 435-474. JSTOR. Retrieved from http://www.jstor.org/stable/43267561.

Ukrainian Journal. (2016, January 12). US DHS probing cyber attack on Oblenergo. *Ukrainian Journal.* Retrieved from http://www.ukrainianjournal.com/index.php?w=article&id=22045

U.S. Congress. (2017). H.R.4718 – 99th Congress: Computer Fraud and Abuse Act of 1986. Retrieved from http://www.congress.gov.

U.S. Congress. (2015a). H.R. 22 – 114th Congress: Fixing America's Surface Transportation Act of 2015. Retrieved from http://www.congress.gov.

U.S. Congress. (2016a). S.2012 – 114th Congress: North American Energy Security and Infrastructure Act of 2016. Retrieved from http://www.congress.gov.

U.S. Congress. (2016b). H.R.2244 – 114th Congress: Strategic Transformer Reserve Program. Retrieved from http://www.congress.gov.

U.S. Congress. (2015b). S.2012 – The Energy Policy Modernization Act. Retrieved from http://www.congress.gov.

U.S. Congress. (2015c). S.1241- Enhanced Grid Security Act of 2015. Retrieved from http://www.congress.gov.

Watts, D. (2003). Security and vulnerability in electric power systems. *North American Power Symposium, 2*, 559-566.

Walker, J., Williams, B. J., & Skelton, G. W. (2010, November). Cybersecurity for emergency management. *Technologies for Homeland Security, Proceedings from the 2010 IEEE International Conference,* 476-480.

WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).

Wu, T. (2013, March 18). Fixing the worst law in technology. *The New Yorker.* Retrieved

from http://www.newyorker.com/online/blogs/newsdesk/2013/03/fixing-the-worst-law-intechnology-aaron-swartz-and-the-computer-fraud-and-abuse-act.html.

Ziska, M. (2017). Integrating cybersecurity into the Incident Command System in an evolving emergency environment (online exclusive). *Disaster Recovery Journal.* Retrieved from https://www.drj.com/articles/online-exclusive/integrating-cybersecurity-into-the-incident-command-system-in-an-evolving-emergency-environment.html

Appendix A: Survey Tool

Introduction

Thank you for participating in this research study. This goal of this study is to understand cybersecurity law and emergency management's relationship with protection of the national electrical grid. The survey is segmented into three sections asking a total of 45 questions that focus on emergency management, cybersecurity law, and electrical grid protection. The survey should only take 5 to 10 minutes to complete and your responses are completely anonymous. If you would like to be considered for a follow-up interview, please provide your contact information at the end of the survey.

Emergency Management

Other (please specify)

1. Your organization is best described as a...*

Investor Owned Utility

Municipal Utility

Not Confident

Somewhat Confident Confident Very Confident N/A

Your utility has an ad hoc emergency management program.

Your utility has an informal undocumented emergency management program.

Your utility has a formal documented emergency management program.

2. Does your utility company have the following?*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

3. Your utility company's emergency management program includes a cybersecurity vulnerability / threat response process.

*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

4. Your utility company's emergency management program includes a preparedness element focused on training, drills, and exercises.

*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

5. Your utility company's emergency management program incorporates the use of the Incident Command System.

*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

6. Your utility company's emergency management program includes plans and procedures for assessing and addressing electric grid vulnerabilities and threats.

*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

7. Your utility company's emergency management program establishes recovery procedures for addressing power loss events affecting the electrical grid.

*

Strongly Disagree Disagree Do no know Agree Strongly Agree N/A

8. Your utility company's emergency management program establishes mitigation measures that lessen the impacts and effects of a power loss event to the electrical grid.

*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

9. Your utility company's emergency management program addresses procedures for both physical and cybersecurity threats/vulnerabilities that could affect the electrical grid.

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

10. Your utility company's threat and vulnerability assessment includes cyber compromising items that could affect the electrical grid such as malware, social engineering, and databreach?

*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

11. Your utility company's emergency management program includes procedures for long term energy emergencies.

*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

12. Your utility company's emergency management program has an integrated cyber-emergency response team.

*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

13. Your utility company's cybersecurity program is a part of your company's overall emergency management program.

*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

14. Your utility company has an established communication plan that coordinates electric grid compromising emergencies with the Electric Sector Coordinating Council.

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

15. Your utility company has an established communication plan that coordinates electric grid compromising emergencies with Federal and State government emergency managment stakeholders.

*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A 16. Your utility company's emergency management program provides protection for the electrical grid.*

Cybersecurity Law

17. I am familiar with the Computer Fraud and Abuse Act.*

Yes

No

Strongly Disagree Disagree Do not know Agree Strongly Agree

18. The Computer Fraud and Abuse Act protects privately owned utilities from external parties that are unauthorized to access your company's computer or network systems.

*

Strongly Disagree Disagree Do not know Agree Strongly Agree

19. The Computer Fraud and Abuse Act only protects Government and Financial sector computer systems from unauthorized parties and internal parties that exceed their computer system authorization.

Strongly Disagree Disagree Do not know Agree Strongly Agree

20. Your Utility company has attempted to use the Computer Fraud and Abuse Act as a measure to deter employees from exceeding their computer system authorization.

Strongly Disagree Disagree Do not know Agree Strongly Agree

21. Your Utility company has attempted to use the Computer Fraud and Abuse Act to deter external unauthorized users from accessing your computer or network systems.

Strongly Disagree Disagree Do not know Agree Strongly Agree

22. Your utility company has attempted to prosecute external unauthorized users criminally for accessing your company's computer or network system.

Strongly Disagree Disagree Do not know Agree Strongly Agree

23. Your utility company has successfully prosecuted external unauthorized computer system users criminally under the Computer Fraud and Abuse Act.

Strongly Disagree Disagree Do not know Agree Strongly Agree 24. The Computer Fraud and Abuse Act protects investor owned utility electric grid critical infrastructure.*

Strongly Disagree Disagree Do not know Agree Strongly Agree 25. I am familiar with the Fixing America's Surface Transportation Act.

Strongly Disagree Disagree Do not know Agree Strongly Agree

26. Your utility company freely shares information about priority critical electric infrastructure with Federal, State, and local government agencies under the Fixing America's Surface Transportation Act.

Strongly Disagree Disagree Do not know Agree Strongly Agree 27. I am familiar with the North American Energy Security and Infrastructure Act of 2016.

Strongly Disagree Disagree Do not know Agree Strongly Agree 28. Your utility company participates in the Strategic Transformer Reserve Plan.

Strongly Disagree Disagree Do not know Agree Strongly Agree 29. Your utility company participates in the Cyber Sense program to protect the electrical grid.

Strongly Disagree Disagree Do not know Agree Strongly Agree

30. The North American Energy Security and Infrastructure Act of 2016 protects the electrical grid from harm.

*

Strongly Disagree Disagree Do not know Agree Strongly Agree 31. I am familiar with the Enhanced Grid Security Act of 2015.

Strongly Disagree Disagree Do not know Agree Strongly Agree 32. Your utility company participates with the Electricity Information Sharing and Analysis Center.

Strongly Disagree Disagree Do not know Agree Strongly Agree

33. The Electricity Information Sharing and Analysis Center provides valuable information that supports your utility to protect the electrical grid from cyber and physical harm.

Strongly Disagree Disagree Do not know Agree Strongly Agree

34. The Enhanced Grid Security Act of 2015 establishes information sharing opportunities to protect the electrical grid from harm.

Electrical Grid Protection & Organizational Information

Not Confident

Somewhat Confident Confident Very Confident N/A

Your company's computer system has been infected with a malware.

Your company can quickly respond to a cybersecurity related emergency that impacts electrical grid.

Your company can stabilize a cybersecurity related emergency that impacts the electrical grid.

Your company can protect its physical industrial control systems from a cybersecurity attack.

35. How confident are you in the following?*

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

An attack on your company's computer system or network could result in real physical consequences, damage to property, and place employees or members of the public in a life safety situation.

Your utility company's cyber emergency response team can quickly detect and respond to a cyber related malware emergency.

36. Would you agree or disagree with the following statements about your utility company's cyber event response capability?

Your utility company's cyber emergency response team has adequate tools to prevent a malware attack from disrupting control center energy management systems.

Your utility company's cyber emergency response program is integrated into your company's physical emergency response program or incident management program.

Your utility company's cyber emergency response team coordinates response efforts with industrial control system operators.

Your utility company's cyber emergency response team has backup communication plan in the event primary communication systems are disrupted during a cyber related incident.

Strongly Disagree Disagree Do not know Agree Strongly Agree N/A

Strongly Disagree Disagree Do not know Agree Strongly Agree

37. Combination of your utility company's Emergency Management program and participation electrical grid security regulations provides a strong strategy for protecting the electrical grid from harm.

Other (please specify)

38. In the last year, our company has experienced_____insider cyber related events.

0

1

10

50

>50

Other (please specify)

39. In the last year, our company has experienced _____ external system penetration attempts.

0

100

500

1000

>1000

Other (please specify)

40. In the last year, our company has experienced _____external system intrusions.

0

20

60

120

>120

41. What is the size of your utility company?

Large (5,000 to 12,000+)

Medium (1000 to 5,000)

Small (<1000)

Other (please specify)

42. What Department of your utility organization do you represent?*

Corporate Services

Operations – Generation

Operations – Distribution

Operations – Transmission

Security Services – Physical Security

Security Services – Cyber Security

Continuity Services

Emergency Management

Other (please specify)

43. What employee level do you represent?

Executive Leadership

Senior Leadership

Director Level Leadership

Mid-Level Management

Front Line Management

44. Which region of the United States does your utility organization serve?

West

Central

Texas

Southeast

Florida

Mid-Atlantic

Northeast

45. If you would like to participate in follow-up interviews, please list your name and contact information.

Appendix B: Integrating Cybersecurity into the Incident Command System in an Evolving Emergency Environment

Ziska, M. (2017). Integrating Cybersecurity into the Incident Command System in an Evolving Emergency Environment. Online Exclusive, 2017 Disaster Recovery Journal. Retrieved from https://www.drj.com/articles/online-exclusive/integrating-cybersecurity-into-the-incident-command-system-in-an-evolving-emergency-environment.html

Abstract

The American threat landscape is changing with the emergence of the cyber threats in the form of malicious software or malware. The United States government is struggling on ways to ensure the nation is prepared to respond to a cyber-related attack that disrupts critical lifeline infrastructure and related systems. New grant opportunities for local and State governments are up-and-coming to assess how cyber-related events should be managed and how cyber response might fit into the National Incident Management System's response framework. The National Incident Management System was adopted in response to the September 11, 2001, attack and has been primarily used for emergencies that impact the physical world. The introduction of malicious software that can cause computer network disruptions can cause real physical consequences to life and property. The Incident Command System responds effectively to the physical aspect of the emergency it may have to evolve to be inclusive of the information technology and cybersecurity professions to manage, investigate, and respond to the cyber threat. This article examines the integration of the cybersecurity function into the Incident Command System providing a blueprint for its inclusivity.

Introduction

Imagine it is the end of the work day and residents of a busy city are going home for the day. The city's power company is in the middle of a shift change, and a control operator employee notices his computer cursor is moving on its own across the screen. The cursor starts to move towards the on-screen breaker controls for substations, and load frequency data begins to show tolerance ranges approaching concerning levels. Substation breakers start to open, and equipment starts to come off line causing a total system failure and mass power outages across the electric distribution network.

This scenario, unfortunately, is not a hypothetical in the technologically dependent world that we live. This scenario is taken directly from what occurred on December 23, 2016, in the Western Ukraine region leaving 230,000 residents without power and heat. What would have happened if bad actors successfully attacked the industrial control systems of a United States power plant, refinery, or local controls such as traffic lights, bridges, or water supplies? How would employees in these sectors organize and manage the response? This article explores the United States response plan using the National Incident Management System's Incident Command System Framework and possible solutions to integrate cybersecurity into the response plan.

National Incident Management System

The World Trade Center attacks on September 11, 2001, drove the United States government to improve coordination of multiple agencies during crisis events initiating the National Incident Management System while adopting the Incident Command System

as the national framework for emergency management (Anderson, 2004). The National Incident Management System is an "All Hazards," governing approach to crisis management with the expectation that each local, State, Federal and nongovernmental organization use this framework to manage emergency events to ensure common response goals are achieved.

The National Incident Management System is comprised of seven components including indoctrination, training, resource management, implementation and reporting, alerts, Federal Emergency Management Agency regional contacts, and the Incident Command System. As previously stated, this article will focus on the Incident Command System. The Incident Command System is a framework that promotes government and nongovernmental organization interoperability when working on small to large scale incidents (Anderson, 2004).

Incident Command System

The Incident Command System first emerged following the 1970 California wildfire season. The wildfire season was devastating to the California landscape and government resources to the extent that communication and support coordination were troubling. In 1972, two years after the devastating wildfires in California, the United States Congress chartered the Firefighting Resources of Southern California Organized for Potential Emergencies (FIRESCOPE) coalition to develop a multi-agency response process to address complex emergencies (Cole, 2000; FEMA, 1987). The FIRESCOPE coalition adjourned providing the nation with a modern emergency management approach and framework.

The Incident Command System is a management structure that simply organizes the response to emergencies. The Incident Command System is structured providing the ability to be fluidly scalable at any point during the lifecycle of an emergency. The Incident Command System is made up a Command Staff and General Staff. The Command Staff consists of the Incident Commander, Public Information Officer, and Safety Officer. The Incident Commander is the individual responsible for every aspect of the emergency response. The Incident Commander has an overarching operational authority and is responsible for developing response strategies, operational tactics, resources, and financial tracking. The Public Information Officer is responsible for incident communications to the outward facing public, media, and community stakeholders. The Safety Officer supports the Incident Commander to assist with the mitigation of situational threats and is responsible for the wellbeing of the emergency responders and the public.

The General Staff of the Incident Command System is comprised of four primary sections. The four major sections are operations, logistics, administration, and finance. These areas are led by section leaders known as “Chiefs” that report directly to the Incident Leader. The four sections can be scaled up or down adding or removing resources given the complexity of a situation.

The Section Chiefs are responsible for executing the tactical operations designated to each section by the Incident Commander. The Operations Chief focuses on actions that support life safety, incident stabilization, and protection of property. The Logistics Chief organizes resources that support the overall incident response operation. The Administrative Chief conducts managerial duties that support tracking and monitoring of personnel time, payment, and schedules while the Finance Chief manages fiduciary responsibility and concerns.

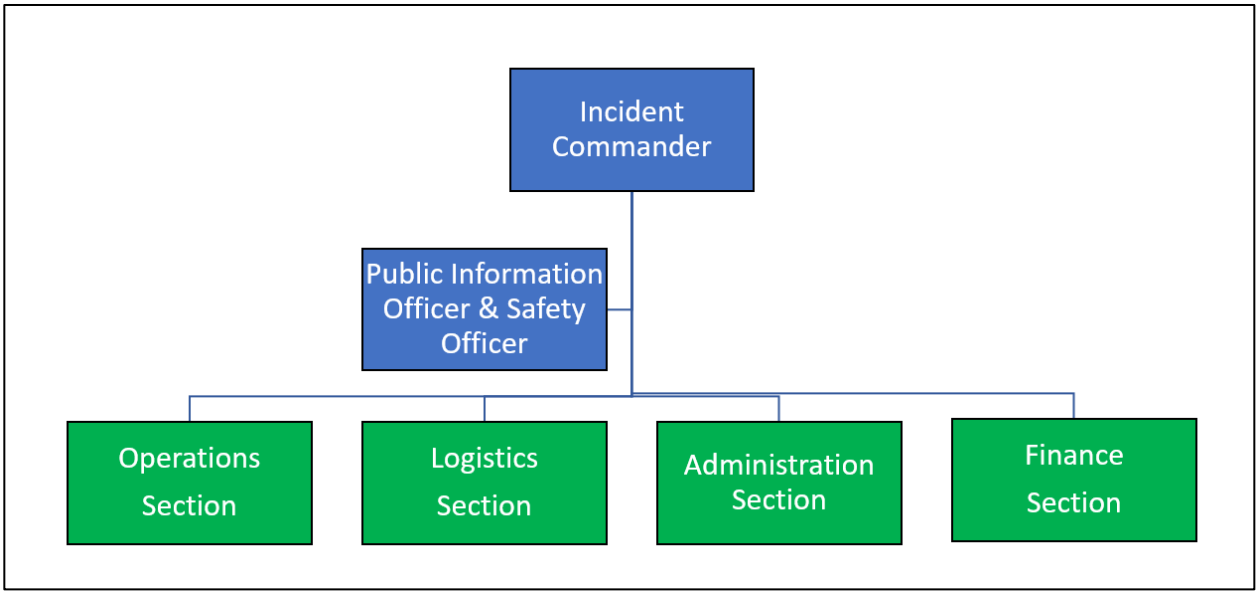

Figure 1 Incident Command System

The Incident Command System is a versatile management structure that organizes incident response no matter how many individuals respond or how many different response agencies participate.

Maturing the Incident Command System

Can the Incident Command System be matured to accommodate a changing threat environment? The short answer is yes. The Incident Command System is structured to be flexible for accommodating an addition to the General Staff for a specific tactical function. In 2013, the Federal government developed guidance to include an intelligence and investigation function into the National Incident Management System's Incident Command System. The intelligence and investigation function was identified as a critical component to collect information surrounding a set of emergency circumstances and therefore was added to the Incident Command System's general staff as seen in figure 2 (Department of Homeland Security, 2013).

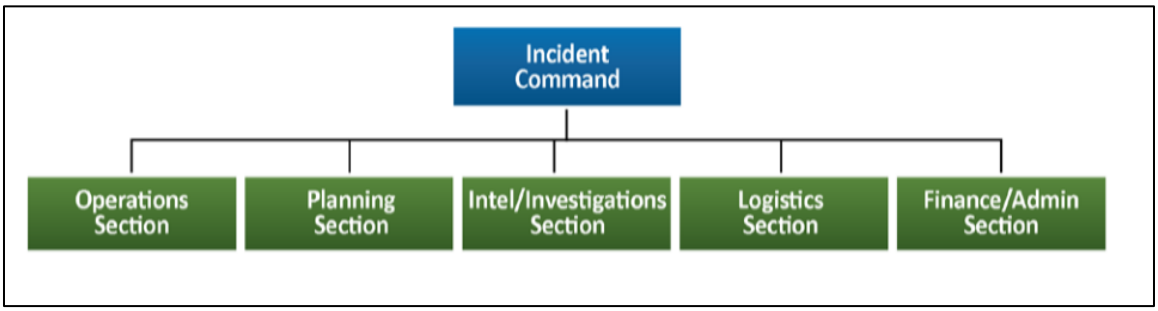

Figure 2 ICS Intel / Investigations Section Structure

The maturation of the Incident Command System to include the intelligence and investigation section was a result of each emergency need to gather critical information to explain the cause, contributing factors, and identify lessons learned (Department of Homeland Security, 2013). The National Preparedness System must continue to adapt to

changing emergency environments to ensure maturation and consistent response goals continue to be attained.

Cybersecurity Function of the Incident Command System

The National Incident Management System's scalability and flexibility allow for a Cybersecurity Function to be integrated into the Incident Command System. The Cybersecurity Function permits for the investigation, information collection, analysis, and sharing of data that could identify the origin of a cyber incident or attack. If the emergency or incident was determined to be the result of a cyber-attack, the Cybersecurity Function would lead the investigation and operational response. If the cyber-attack were determined to be a criminal act, the Cybersecurity Function would share the information with the proper operational enforcement authorities.

In today's cyber threat environment, emergency response personnel should consider a potential cyber incident as a potential cause of an incident and take necessary action to determine causality while upholding the response objectives to protect life, stabilize the incident, and protect property. The Cybersecurity Function should be integrated into the Incident Command System to efficiently detect and respond to cybersecurity threats that potentially cause emergencies that have real physical consequences such as the disruption of industrial control systems, network systems, energy systems, transportation systems, or any disruption of lifeline critical infrastructure.

The Cybersecurity Function should be installed in the General Staff Section of the Incident Command System when a critical infrastructure system is associated with an

incident as shown in figure 3. The function may be combined with other general staff sections to form task force operations to understand the nature of the incident further,

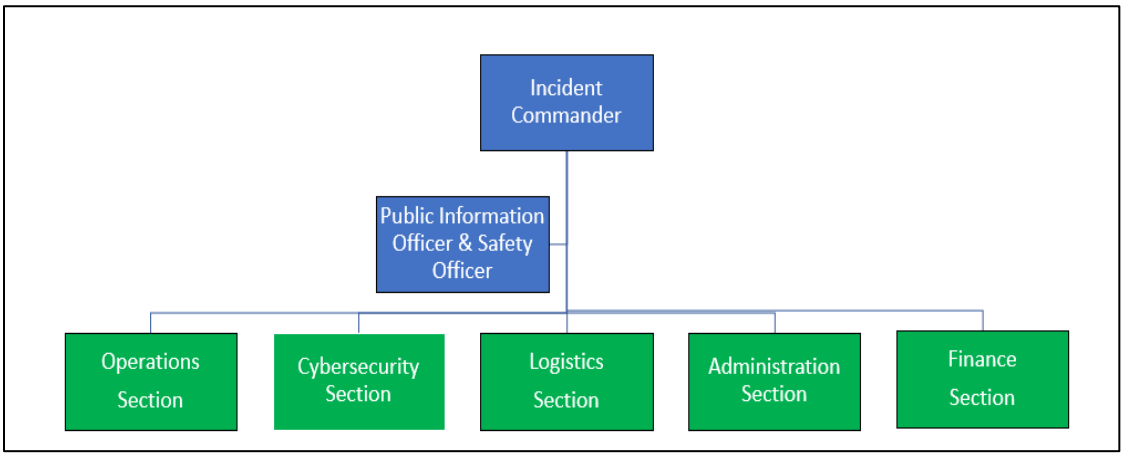

Figure 3 Cybersecurity Section of the Incident Command System

share information and ensure primary response objectives are completed.

How would Cybersecurity Participate in Preparedness Activities?

The Cybersecurity Function, before the beginning of an incident, could be used to attain system data, conduct penetration testing, and address identified system vulnerabilities. The Cybersecurity Function could establish a centralized information monitoring center to identify system threats that could potentially affect Internet dependent systems such as supervisory control and data acquisition (SCADA) systems and industrial control systems. Preparedness activities could include planning for a cyber related response, information sharing, coordination with intelligence agencies, and transferring information evidence for criminal investigation by enforcement authorities.

Cybersecurity Function Organization

The National Incident Management System is organized into Branches, Groups, and Divisions to ensure proper incident scalability. The Cybersecurity Function could be organized into Groups that represent various mission areas. The Cybersecurity Function Section Chief would be responsible for increasing the span of control activating Groups when necessary. The Groups' activation would be based on the needs and scope of the incident and could include:

- **Analyst Group:** Provide tactical and strategic level analysis of cyber threats, vectors, and actors supporting the defense of computer network operations.
- **Forensic Group:** Provide forensic analysis of computer network operations to investigate data, preserve malicious data as evidence, and determine routes of the system or network entry.
- **Intelligence Group:** Monitor computer network systems and other data sources to predict nefarious cyber actor behaviors, determine if threats are credible, share information with other organizations, and develop situation reports.

- **Data Evidence Group:** Manage preserved data evidence and share it with agencies or organizations for future criminal prosecution.

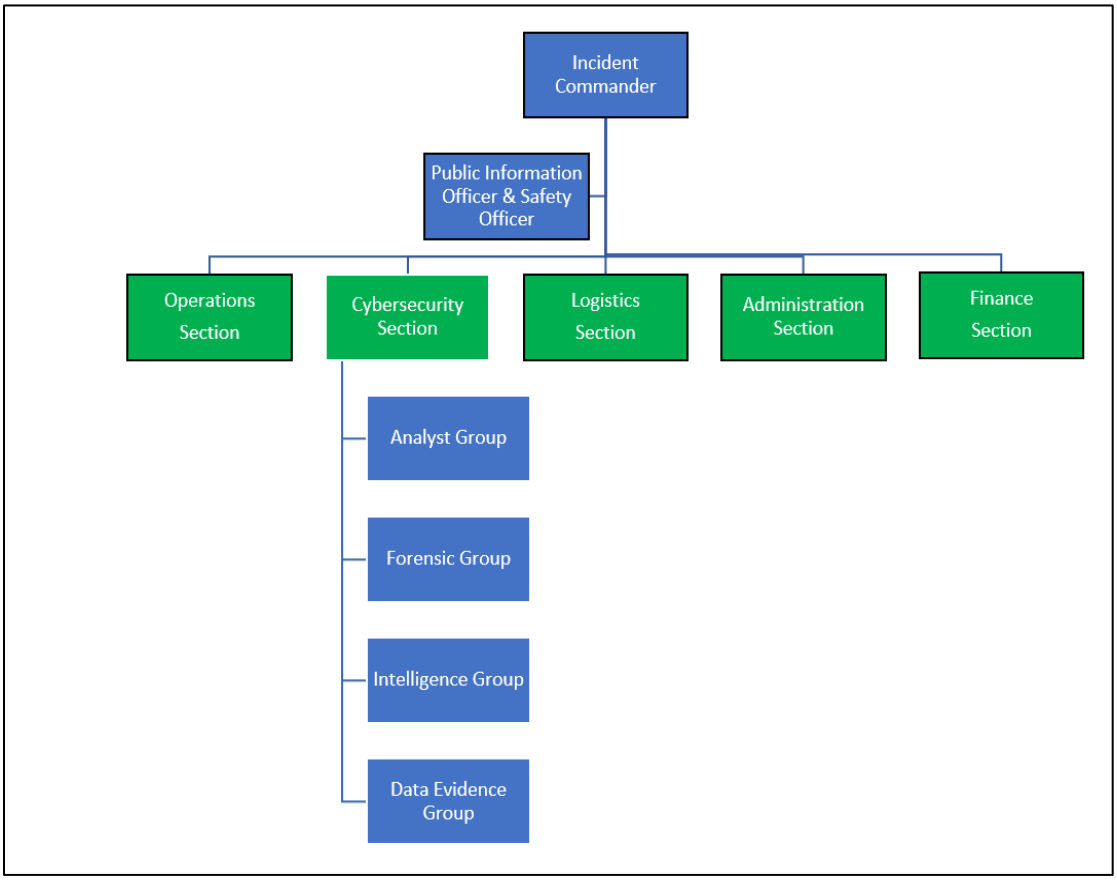

Figure 4 Cybersecurity Groups

Summary

The Cybersecurity Function as an addition to the Incident Command System aligns with the National Incident Management System's mission to provide a flexible and scalable framework for incident response. The integration of a Cybersecurity Function could provide enhanced situational awareness, information sharing, and tactical cyber defense operations during an incident where a cyber-attack is suspected. The function is

necessary when a critical infrastructure fails and should be activated by the Incident Commander to contribute to the situational awareness and investigation of the event.

Appendix C: Presidential Policy Directive 41 United States Cyber Incident Coordination

PRESIDENTIAL POLICY DIRECTIVE/PPD-41

SUBJECT: United States Cyber Incident Coordination

The advent of networked technology has spurred innovation, cultivated knowledge, encouraged free expression, and increased the Nation's economic prosperity. However, the same infrastructure that enables these benefits is vulnerable to malicious activity, malfunction, human error, and acts of nature, placing the Nation and its people at risk. Cyber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency, impacting public and private infrastructure located in the United States and abroad.

United States preparedness efforts have positioned the Nation to manage a broad range of threats and hazards effectively. Every day, Federal law enforcement and those agencies responsible for network defense in the United States manage, respond to, and investigate cyber incidents in order to ensure the security of our information and communications infrastructure. The private sector and government agencies have a shared vital interest in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences. The nature of cyberspace requires individuals, organizations, and the government to all play roles in incident response. Furthermore, effective incident response efforts will help support an open, interoperable, secure, and reliable information and communications infrastructure that promotes trade and commerce, strengthens

international security, fosters free expression, and reinforces the privacy and security of our citizens.

While the vast majority of cyber incidents can be handled through existing policies, certain cyber incidents that have significant impacts on an entity, our national security, or the broader economy require a unique approach to response efforts. These significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors.

I. Scope

This Presidential Policy Directive (PPD) sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. For significant cyber incidents, this PPD also establishes lead Federal agencies and an architecture for coordinating the broader Federal Government response. This PPD also requires the Departments of Justice and Homeland Security to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities.

II. Definitions

Cyber incident. An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an

information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Significant cyber incident. A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

III. Principles Guiding Incident Response

In carrying out incident response activities for any cyber incident, the Federal Government will be guided by the following principles:

Shared Responsibility. Individuals, the private sector, and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.

Risk-Based Response. The Federal Government will determine its response actions and the resources it brings to bear based on an assessment of the risks posed to an entity, our national security, foreign relations, the broader economy, public confidence, civil liberties, or the public health and safety of the American people.

Respecting affected entities. To the extent permitted under law, Federal Government responders will safeguard details of the incident, as well as privacy and civil liberties, and sensitive private sector information, and generally will defer to affected entities in notifying other affected private sector entities and the public. In the event a significant Federal Government interest is served by issuing a public statement concerning an

incident, Federal responders will coordinate their approach with the affected entities to the extent possible.

Unity of Governmental Effort. Various government entities possess different roles, responsibilities, authorities, and capabilities that can all be brought to bear on cyber incidents. These efforts must be coordinated to achieve optimal results. Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right combination of agencies responds to a particular incident. State, local, tribal, and territorial (SLTT) governments also have responsibilities, authorities, capabilities, and resources that can be used to respond to a cyber incident; therefore, the Federal Government must be prepared to partner with SLTT governments in its cyber incident response efforts. The transnational nature of the Internet and communications infrastructure requires the United States to coordinate with international partners, as appropriate, in managing cyber incidents.

Enabling Restoration and Recovery. Federal response activities will be conducted in a manner to facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and national security requirements, public health and safety, and the need to return to normal operations as quickly as possible.

IV. Concurrent Lines of Effort

In responding to any cyber incident, Federal agencies shall undertake three concurrent lines of effort: threat response; asset response; and intelligence support and related activities. In addition, when a Federal agency is an affected entity, it shall undertake a

fourth concurrent line of effort to manage the effects of the cyber incident on its operations, customers, and workforce.

Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.

Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.

Threat and asset responders will share some responsibilities and activities, which may include communicating with affected entities to understand the nature of the cyber incident; providing guidance to affected entities on available Federal resources and capabilities; promptly disseminating through appropriate channels intelligence and information learned in the course of the response; and facilitating information sharing and operational coordination with other Federal Government entities.

Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.

An affected Federal agency shall engage in a variety of efforts to manage the impact of a cyber incident, which may include maintaining business or operational continuity; addressing adverse financial impacts; protection of privacy; managing liability risks; complying with legal and regulatory requirements (including disclosure and notification); engaging in communications with employees or other affected individuals; and dealing with external affairs (e.g., media and congressional inquiries). The affected Federal agency will have primary responsibility for this line of effort.

When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity. The relevant sector-specific agency (SSA) will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

V. Architecture of Federal Government Response Coordination for Significant Cyber Incidents1

In order to respond effectively to significant cyber incidents, the Federal Government will coordinate its activities in three ways:

National Policy Coordination 2

The Cyber Response Group (CRG), in support of the National Security Council (NSC) Deputies and Principals Committees, and accountable through the Assistant to the President for Homeland Security and Counterterrorism (APHSCT) to the NSC chaired by the President, shall coordinate the development and implementation of United States Government policy and strategy with respect to significant cyber incidents affecting the United States or its interests abroad.

National Operational Coordination

Agency Enhanced Coordination Procedures. Each Federal agency that regularly participates in the CRG, including SSAs, shall establish and follow enhanced coordination procedures as defined in the annex to this PPD in situations in which the demands of responding to a significant cyber incident exceed its standing capacity.

Cyber Unified Coordination Group. A Cyber Unified Coordination Group (UCG) shall serve as the primary method for coordinating between and among Federal agencies in response to a significant cyber incident as well as for integrating private sector partners into incident response efforts, as appropriate. A Cyber UCG shall be formed at the direction of the NSC Principals Committee, Deputies Committee, or the CRG, or when two or more Federal agencies that generally participate in the CRG, including relevant SSAs, request its formation. A Cyber UCG shall also be formed when a significant cyber incident affects critical infrastructure owners and operators identified by the Secretary of Homeland Security as owning or operating critical infrastructure for which a cyber incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

A Cyber UCG will normally consist of Federal lead agencies for threat response, asset response, and intelligence support, but will also include SSAs, if a cyber incident affects or is likely to affect sectors they represent. In addition, as required by the scope, nature, and facts of a particular significant cyber incident, a Cyber UCG may include participation from other Federal agencies, SLTT governments, nongovernmental organizations, international counterparts, or the private sector.

Following the formation of a Cyber UCG, Federal agencies responding to the incident shall assign appropriate senior executives, staff, and resources to execute the agency's responsibilities as part of a Cyber UCG. The Cyber UCG is intended to result in unity of effort and not to alter agency authorities or leadership, oversight, or command responsibilities. Unless mutually agreed upon between agency heads or their designees, and consistent with applicable legal authorities such as the Economy Act of 1932 (31 U.S.C. 1535), Federal departments and agencies will maintain operational control over their respective agency assets.

Federal lead agencies. In order to ensure that the Cyber UCG achieves maximum effectiveness in coordinating responses to significant cyber incidents, the following agencies shall serve as Federal lead agencies for the specified line of effort:

In view of the fact that significant cyber incidents will often involve at least the possibility of a nation-state actor or have some other national security nexus, the Department of Justice, acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, shall be the Federal lead agency for threat response activities.

The Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, shall be the Federal lead agency for asset response activities.

The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, shall be the Federal lead agency for intelligence support and related activities.

Drawing upon the resources and capabilities across the Federal Government, the Federal lead agencies are responsible for:

Coordinating any multi-agency threat or asset response activities to provide unity of effort, to include coordinating with any agency providing support to the incident, to include SSAs in recognition of their unique expertise;

Ensuring that their respective lines of effort are coordinated with other Cyber UCG participants and affected entities, as appropriate;

Identifying and recommending to the CRG, if elevation is required, any additional Federal Government resources or actions necessary to appropriately respond to and recover from the incident; and

Coordinating with affected entities on various aspects of threat, asset, and affected entity response activities through a Cyber UCG, as appropriate.

Field-Level Coordination

Field-level representatives of the Federal asset or threat response lead agencies shall ensure that they effectively coordinate their activities within their respective lines of

effort with each other and the affected entity. Such representatives may be co-located with the affected entity.

VI. Unified Public Communications

The Departments of Homeland Security and Justice shall maintain and update as necessary a fact sheet outlining how private individuals and organizations can contact relevant Federal agencies about a cyber incident.

VII. Relationship to Existing Policy

Nothing in this directive alters, supersedes, or limits the authorities of Federal agencies to carry out their functions and duties consistent with applicable legal authorities and other Presidential guidance and directives. This directive generally relies on and furthers the implementation of existing policies and explains how United States cyber incident response structures interact with those existing policies. In particular, this policy complements and builds upon PPD-8 on National Preparedness of March 30, 2011. By integrating cyber and traditional preparedness efforts, the Nation will be ready to manage incidents that include both cyber and physical effects.

BARACK OBAMA

Appendix D: Strengthening Cybersecurity of Federal Networks and Critical Infrastructure

EXECUTIVE ORDER

- - - - - - -

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to protect American innovation and values, it is hereby ordered as follows:

Section 1. Cybersecurity of Federal Networks.

(a) Policy. The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

(b) Findings.

(i) Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents. Information sharing facilitates and supports all of these activities.

(ii) The executive branch has for too long accepted antiquated and difficult–to-defend IT.

(iii) Effective risk management involves more than just protecting IT and data currently in place. It also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity.

(iv) Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies (agencies). Known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance.

(v) Effective risk management requires agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources.

(c) Risk Management.

(i) Agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction

of IT and data. They will also be held accountable by the President for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes, in accordance with chapter 35, subchapter II of title 44, United States Code.

(ii) Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk. Each agency head shall provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) within 90 days of the date of this order. The risk management report shall:

(A) document the risk mitigation and acceptance choices made by each agency head as of the date of this order, including:

(1) the strategic, operational, and budgetary considerations that informed those choices; and

(2) any accepted risk, including from unmitigated vulnerabilities; and

(B) describe the agency's action plan to implement the Framework.

(iii) The Secretary of Homeland Security and the Director of OMB, consistent with chapter 35, subchapter II of title 44, United States Code, shall jointly assess each agency's risk management report to determine whether the risk mitigation and acceptance choices set forth in the reports are appropriate and sufficient to manage the cybersecurity risk to the executive branch enterprise in the aggregate (the determination).

(iv) The Director of OMB, in coordination with the Secretary of Homeland Security, with appropriate support from the Secretary of Commerce and the Administrator of General Services, and within 60 days of receipt of the agency risk management reports outlined in subsection (c)(ii) of this section, shall submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the following:

(A) the determination; and

(B) a plan to:

(1) adequately protect the executive branch enterprise, should the determination identify insufficiencies;

(2) address immediate unmet budgetary needs necessary to manage risk to the executive branch enterprise;

(3) establish a regular process for reassessing and, if appropriate, reissuing the determination, and addressing future, recurring unmet budgetary needs necessary to manage risk to the executive branch enterprise;

(4) clarify, reconcile, and reissue, as necessary and to the extent permitted by law, all policies, standards, and guidelines issued by any agency in furtherance of chapter 35, subchapter II of title 44, United States Code, and, as necessary and to the extent permitted by law, issue policies, standards, and guidelines in furtherance of this order; and

(5) align these policies, standards, and guidelines with the Framework.

(v) The agency risk management reports described in subsection (c)(ii) of this section and the determination and plan described in subsections (c)(iii) and (iv) of this section may be classified in full or in part, as appropriate.

(vi) Effective immediately, it is the policy of the executive branch to build and maintain a modern, secure, and more resilient executive branch IT architecture.

(A) Agency heads shall show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services.

(B) The Director of the American Technology Council shall coordinate a report to the President from the Secretary of Homeland Security, the Director of OMB, and the Administrator of General Services, in consultation with the Secretary of Commerce, as appropriate, regarding modernization of Federal IT. The report shall:

(1) be completed within 90 days of the date of this order; and

(2) describe the legal, policy, and budgetary considerations relevant to -- as well as the technical feasibility and cost effectiveness, including timelines and milestones, of -- transitioning all agencies, or a subset of agencies, to:

(aa) one or more consolidated network architectures; and

(bb) shared IT services, including email, cloud, and cybersecurity services.

(C) The report described in subsection (c)(vi)(B) of this section shall assess the effects of transitioning all agencies, or a subset of agencies, to shared IT services with respect to cybersecurity, including by making recommendations to ensure consistency with section 227 of the Homeland Security Act (6 U.S.C. 148) and compliance with policies and practices issued in accordance with section 3553 of title 44, United States Code. All agency heads shall supply such information concerning their current IT architectures and plans as is necessary to complete this report on time.

(vii) For any National Security System, as defined in section 3552(b)(6) of title 44, United States Code, the Secretary of Defense and the Director of National Intelligence, rather than the Secretary of Homeland Security and the Director of OMB, shall implement this order to the maximum extent feasible and appropriate. The Secretary of Defense and the Director of National Intelligence shall provide a report to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism describing their implementation of subsection (c) of this section within 150 days of the date of this order. The report described in this subsection shall include a justification for any deviation from the requirements of subsection (c), and may be classified in full or in part, as appropriate.

Sec. 2. Cybersecurity of Critical Infrastructure.

(a) Policy. It is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure (as defined in section 5195c(e) of title 42, United States Code) (critical infrastructure entities), as appropriate.

(b) Support to Critical Infrastructure at Greatest Risk. The Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the heads of appropriate sector-specific agencies, as defined in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience) (sector-specific agencies), and all other appropriate agency heads, as identified by the Secretary of Homeland Security, shall:

(i) identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities);

(ii) engage section 9 entities and solicit input as appropriate to evaluate whether and how the authorities and capabilities identified pursuant to subsection (b)(i) of this section might be employed to support cybersecurity risk management efforts and any obstacles to doing so;

(iii) provide a report to the President, which may be classified in full or in part, as appropriate, through the Assistant to the President for Homeland Security and Counterterrorism, within 180 days of the date of this order, that includes the following:

(A) the authorities and capabilities identified pursuant to subsection (b)(i) of this section;

(B) the results of the engagement and determination required pursuant to subsection (b)(ii) of this section; and

(C) findings and recommendations for better supporting the cybersecurity risk management efforts of section 9 entities; and

(iv) provide an updated report to the President on an annual basis thereafter.

(c) Supporting Transparency in the Marketplace. The Secretary of Homeland Security, in coordination with the Secretary of Commerce, shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, that

examines the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities, within 90 days of the date of this order.

(d) Resilience Against Botnets and Other Automated, Distributed Threats. The Secretary of Commerce and the Secretary of Homeland Security shall jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets). The Secretary of Commerce and the Secretary of Homeland Security shall consult with the Secretary of Defense, the Attorney General, the Director of the Federal Bureau of Investigation, the heads of sector-specific agencies, the Chairs of the Federal Communications Commission and Federal Trade Commission, other interested agency heads, and appropriate stakeholders in carrying out this subsection. Within 240 days of the date of this order, the Secretary of Commerce and the Secretary of Homeland Security shall make publicly available a preliminary report on this effort. Within 1 year of the date of this order, the Secretaries shall submit a final version of this report to the President.

(e) Assessment of Electricity Disruption Incident Response Capabilities. The Secretary of Energy and the Secretary of Homeland Security, in consultation with the Director of National Intelligence, with State, local, tribal, and territorial governments, and with others as appropriate, shall jointly assess:

(i) the potential scope and duration of a prolonged power outage associated with a significant cyber incident, as defined in Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination), against the United States electric subsector;

(ii) the readiness of the United States to manage the consequences of such an incident; and

(iii) any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident.

The assessment shall be provided to the President, through the Assistant to the President for Homeland Security and Counterterrorism, within 90 days of the date of this order, and may be classified in full or in part, as appropriate.

(f) Department of Defense Warfighting Capabilities and Industrial Base. Within 90 days of the date of this order, the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation, in coordination with the Director of National Intelligence, shall provide a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks. The report may be classified in full or in part, as appropriate.

Sec. 3. Cybersecurity for the Nation.

(a) Policy. To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure

internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.

(b) Deterrence and Protection. Within 90 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, and the United States Trade Representative, in coordination with the Director of National Intelligence, shall jointly submit a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats.

(c) International Cooperation. As a highly connected nation, the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners toward maintaining the policy set forth in this section. Within 45 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Secretary of Commerce, and the Secretary of Homeland Security, in coordination with the Attorney General and the Director of the Federal Bureau of Investigation, shall submit reports to the President on their international cybersecurity priorities, including those concerning investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation. Within 90 days of the

submission of the reports, and in coordination with the agency heads listed in this subsection, and any other agency heads as appropriate, the Secretary of State shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, documenting an engagement strategy for international cooperation in cybersecurity.

(d) Workforce Development. In order to ensure that the United States maintains a long-term cybersecurity advantage:

(i) The Secretary of Commerce and the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Secretary of Labor, the Secretary of Education, the Director of the Office of Personnel Management, and other agencies identified jointly by the Secretary of Commerce and the Secretary of Homeland Security, shall:

(A) jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and

(B) within 120 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.

(ii) The Director of National Intelligence, in consultation with the heads of other agencies identified by the Director of National Intelligence, shall:

(A) review the workforce development efforts of potential foreign cyber peers in order to help identify foreign workforce development practices likely to affect long-term United States cybersecurity competitiveness; and

(B) within 60 days of the date of this order, provide a report to the President through the Assistant to the President for Homeland Security and Counterterrorism on the findings of the review carried out pursuant to subsection (d)(ii)(A) of this section.

(iii) The Secretary of Defense, in coordination with the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence, shall:

(A) assess the scope and sufficiency of United States efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities; and

(B) within 150 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations on the assessment carried out pursuant to subsection (d)(iii)(A) of this section.

(iv) The reports described in this subsection may be classified in full or in part, as appropriate.

Sec. 4. Definitions. For the purposes of this order:

(a) The term "appropriate stakeholders" means any non-executive-branch person or entity that elects to participate in an open and transparent process established by the Secretary of Commerce and the Secretary of Homeland Security under section 2(d) of this order.

(b) The term "information technology" (IT) has the meaning given to that term in section 11101(6) of title 40, United States Code, and further includes hardware and software systems of agencies that monitor and control physical equipment and processes.

(c) The term "IT architecture" refers to the integration and implementation of IT within an agency.

(d) The term "network architecture" refers to the elements of IT architecture that enable or facilitate communications between two or more IT assets.

Sec. 5. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be construed to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence or law enforcement operations.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP

THE WHITE HOUSE,

May 11, 2017.

Appendix E: Proposed Amended Language to the Computer Fraud and Abuse Act

Proposed language changes are underlined.

(a)Whoever—

(1)having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national sustainability, national defense, or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States;

(C) information from any private or non-government organization responsible for owning and or operating systems critical to the sustainability of the United States as defined as Critical Infrastructure; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B)intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C)intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[2]

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A)such trafficking affects interstate or foreign commerce; or

(B)such computer is used by or for the Government of the United States; [3]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b)Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B)a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A)a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B)a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),[4] or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)

(A)except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—

(i)an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

(I)loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more <u>critical infrastructure computers</u> or other protected computers) aggregating at least $5,000 in value;

(II)the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III)physical injury to any person;

(IV)a threat to public health or safety;

(V)damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national sustainability, national defense, or national security; or

(VI)damage affecting 10 or more computers used to operate critical infrastructure or protected computers during any 1-year period; or

(ii)an attempt to commit an offense punishable under this subparagraph;

(B)except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i)an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii)an attempt to commit an offense punishable under this subparagraph;

(C)except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of—

(i)an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii)an attempt to commit an offense punishable under this subparagraph;

(D)a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i)an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or

(ii)an attempt to commit an offense punishable under this subparagraph;

(E)if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F)if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G)a fine under this title, imprisonment for not more than 1 year, or both, for—

(i)any other offense under subsection (a)(5); or

(ii)an attempt to commit an offense punishable under this subparagraph.

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2)The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national sustainability, national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e)As used in this section—

(1) the term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2)the term “protected computer” means a computer—

(A)exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B)which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3)the term “State” includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4)the term “financial institution” means—

(A)an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B)the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C)a credit union with accounts insured by the National Credit Union Administration;

(D)a member of the Federal home loan bank system and any home loan bank;

(E)any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F)a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G)the Securities Investor Protection Corporation;

(H)a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I)an organization operating under section 25 or section 25(a) 1 of the Federal Reserve Act;

(5)the term “financial record” means information derived from any record held by a financial institution pertaining to a customer’s relationship with the financial institution;

(6)the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7)the term “department of the United States” means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8)the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information;

(9)the term “government entity” includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10)the term “conviction” shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11)the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service;

(12) the term “Critical Infrastructure” means essential services that underpin American Society owned and operated by the United States government, private sector, and non-government organizations to strengthen and maintain secure, functioning, and resilient assets, networks, and systems vital to the Nation’s safety, prosperity, and well-being as defined in Presidential Policy Directive 21, Homeland Security Presidential Directive 7, and Homeland Security Critical Infrastructure Sectors.

(13) the term “person” means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f)This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g)Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may

be brought only if the conduct involves 1 of the factors set forth in subclauses [5] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h)The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i)

(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

(A)such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B)any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2)The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the

provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j)For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1)Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2)Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section [6]