CERIAS Tech Report 2008-16

Status Report on Cyber Critical Infrastructure Protection Involving the Bulk-Power Grid System

by Marianne Hoebich
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

STATUS REPORT ON CYBER CRITICAL INFRASTRUCTURE PROTECTION INVOLVING THE BULK-POWER GRID SYSTEM

A Thesis

Submitted to the Faculty

of

Purdue University

by

Marianne Hoebich

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

May 2008

Purdue University

West Lafayette, Indiana

ACKNOWLEDGMENTS

The author would like to thank Dr. Marcus Rogers, Dr. Victor Raskin, Dr. Eugene Spafford, and Marlene Walls for their advice, patience, and humor. Without them my stay at Purdue University would have been greatly diminished.

TABLE OF CONTENTS

Page

Page

Page

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

CEII	Critical Energy Infrastructure Information
CIP	Critical Infrastructure Protection
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
EIA	Energy Information Administration
EPA	Energy Policy Act of 2005
ERO	Electric Reliability Organization
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
FBI	Federal Bureau of Investigations
FERC	Federal Energy Regulatory Commission
GAO	US Government Accountability Office
HSPD-7	Homeland Security Presidential Directive 7
ISAC	Information Sharing and Analysis Center
NERC	North American Electric Reliability Corporation
NIPP	National Plan for Infrastructure Protection
PCCIP	President's Commission of Critical Infrastructure Protection
PCII	Protected Critical Infrastructure Information
PDD 63	Presidential Decision Directive 63
SCADA	Supervisory Control and Data Acquisition
TCP/IP	Transmission Control Protocol (TCP) and the Internet Protocol (IP)
UA-1200	Urgent Action Standard 1200 – Cyber Security

ABSTRACT

Hoebich, Marianne. M.S., Purdue University, May, 2008. Status Report On Cyber Critical Infrastructure Protection Involving the Bulk-Power Grid System. Major Professor: Dr. Marcus Rogers.

This research report provides a historical perspective on key developments in cyber critical infrastructure protection efforts to secure the bulk-power grid system. It is important to understand the past so future efforts can benefit from the knowledge gained from past experiences. The research examines 21 key developments that occur from 1997 to 2008. The developments are sorted into three groups: DHS (represents public sector), NERC (representing the private sector), and FERC (regulatory function). The developments within each group are then analyzed to identify what prior developments contributed to later developments. The main underlying theme in each group is also examined to identify potential issues that hinder cyber critical infrastructure protection efforts. The results of this research show that some progress has been made by the combined efforts of NERC and FERC. The DHS has produced plans but has been unable to effectively implement those plans. The three main issues that were identified are the impact of economics, major power outages, and the ineffective partnership efforts between the DHS and the private entities within the electricity sector. These issues will need to be solved in the future so cyber critical infrastructure protection for the bulk-power grid system can proceed.

CHAPTER 1. THE PROBLEM

1.1. Introduction

Reliable critical infrastructure services are required for a society and its economy to function effectively. One of the critical infrastructures in the United States is the bulk-power grid system. This system is responsible for the generation and distribution of electricity within the United States.

The bulk-power grid system consists of physical and cyber components. The cyber components (also referred to as cyber critical infrastructure) consist of computer systems, control systems, and communication systems. The cyber critical infrastructure manages and controls the physical components of the bulk-power grid system. The physical components consist of high-voltage transformers, generators, and high-voltage wires, used for the generation and distribution of electricity.

The adoption on commonly used, off-the-shelf, information technology products and the Internet in the electricity sector's critical infrastructure, has made the bulk-power grid system susceptible to cyber-based attacks (Government Accountability Office [GAO], 2007c). Over the last 11 years there have been several key developments in cyber critical infrastructure protection by Department of Homeland Security (DHS), Department of Energy (DOE), the North American Reliability Corporation (NERC), and the United States Federal Energy Regulatory Commission (FERC). Examining these developments will provide a more complete perspective on the status of current cyber critical infrastructure protection in the electricity sector and help identify underlying issues that inhibit progress.

1.2. Statement of the Problem

In order to have a better understanding of cyber critical infrastructure protection efforts in the bulk-power grid system, it is important to examine the key developments that have occurred over at least a ten year period of time. This provides perspective that is not achieved when analyzing events over a short time period. In this research the developments spanned an 11 year timeframe. Understanding the context of these developments provides a clear picture of the status of critical infrastructure protection in the electricity sector.

The problem addressed by this research is the lack of collected, related information on cyber critical infrastructure protection developments involving DHS, DOE, NERC, and FERC that contributes to the current status of securing the bulk-power grid system from cyber attacks.

1.3. Significance of the Problem

In order to secure the bulk-power grid system from cyber attacks it is important to understand what has happened in the past. Future efforts at cyber critical infrastructure protection should be based on the knowledge gained from past experiences.

1.4. Purpose of the Research

The purpose of this research is to provide a historical perspective on key developments in cyber critical infrastructure protection efforts to secure the bulk-power grid system from cyber attacks and to identify impeding issues, so that future efforts can learn from previous efforts. The research is meant to provide a high-level understanding of efforts to secure the bulk-power grid system from cyber attacks.

1.5. Delimitations

Due to the vast amounts of information available on this subject area and the timeline spanning eleven years, several conditions were set to restrict the scope of the research.

The cyber critical infrastructure protection developments examined in this report are confined to efforts by DHS, DOE, NERC, and FERC. These organizations are the main participants in cyber critical infrastructure protection efforts involving the bulk-power grid system.

The literature reviewed and processed in this research came solely from Internet sources. The main sources of literature come from the following Web sites:

- DHS
- DOE
- NERC
- FERC
- The White House
- Government Accountability Office (GAO)

The timeline for developments regarding cyber critical infrastructure protection in the electricity sector is restricted from 1997 to 2008. The developments selected over this timeframe are restricted to a group of less than 25 key developments. This provides enough perspective to determine the current status of cyber critical infrastructure protection efforts. Additionally, only themes/issues that appear continuously throughout the eleven year time period are examined and only three are included in this research report.

1.6. Limitations

This research is based on Internet sources. Even though over 60 reports were reviewed in this research effort, it is possible that the reports do not portray an accurate picture of cyber critical infrastructure protection for the electricity

sector. However, the number of documents processed reveals a relatively accurate picture of the situation. However, the impact of this limitation could provide an inaccurate picture of cyber critical infrastructure protection.

1.7. Definitions

The following definitions explain key terms used in this research paper.

- Bulk-power grid system – this includes generation, transmission, distribution, network computer controls, and information technology protection systems, used to provide the reliable, continuous flow of electricity in the US (Energy Policy Act, 2005).
- Critical infrastructure – “Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government (The White House, 1998, ¶3). Critical Infrastructure consists of assets, systems, and networks, which if disrupted would have a debilitating impact on the economy, security, and public health of the country. Critical Infrastructure consists of telecommunications, energy (e.g., power generation and distribution), banking, transportation, healthcare services, water systems, and emergency services (Department of Homeland Security [DHS], 2006a).
- Critical infrastructure information – “means information not customarily in the public domain and related to the security of critical infrastructure or protected systems” (Homeland Security Act [HSA], 2002, p. 17). This information could be used to find or exploit a vulnerability of the critical infrastructure service that could potentially compromise or incapacitate that service.
- Critical infrastructure protection – the measures taken to protect critical infrastructure from perceived and real threats.

- Cyber attack – an attack that utilizes electronic medium to incapacitate or disrupt an electronic service, such as a network, information technology system, and /or communication system. The attack focuses on violating the confidentiality, integrity, and or the availability of the computer system and the services it provides. “A discrete malicious action of debilitating intent inflicted by one entity upon another” (President’s Commission on Critical Infrastructure Protection [PCCIP], 1997, p.B-1).
- Cyber critical infrastructure – is made up of hardware and software information technology products and the data contained in them used to manage and control operations of the physical critical infrastructure. Cyber critical infrastructure also consists of the networks and systems used to communicate, process, and store electronic data and information (DHS, 2006a).
- Cyber critical infrastructure protection – consist of the effort to secure the cyber critical infrastructure from cyber attacks and to reduce vulnerabilities and threats to cyber critical infrastructure.
- Cyber security – efforts taken to ensure confidentiality, integrity, and availability of electronic information or data from malicious activities such as unauthorized access, manipulation, and destruction (DHS, 2006a).
- Entities – Reliability coordinators, balancing authorities, interchange authorities, transmission service providers, transmission owners, transmission operators, generator owners, generator operators, load serving entities, NERC, and regional reliability organizations (United States of America Federal Energy Regulatory Commission [FERC], 2008a).
- Public-private partnership – “A relationship between two or more entities wherein each accepts responsibility to contribute a

specified, but not necessarily equal, level of effort to the achievement of a common goal" (PCCIP, 1997, p. B-3).

- Reliability standards – FERC approved requirement that when implemented enables reliable operation of the bulk-power grid system (Energy Policy Act, 2005).
- Supervisory Control and Data Acquisition (SCADA) – These computer systems are used in utility infrastructures to monitor, control, collect, and store data from remotely-located devices, such as transducers and sensors. There purpose is to monitor and control equipment based upon data received from remote devices (Scandia Corporation, n.d.).
- Threat – The intention and capability of an adversary to undertake actions that would be detrimental to critical infrastructure (DHS, 2006a).
- Vulnerability – "A characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat" (PCCIP, 1997, p. B-3).

CHAPTER 2. LITERATURE REVIEW

2.1. Cyber Attacks and the Bulk-Power Grid System

The bulk-power grid system is one of the critical infrastructures of the United States that is vulnerable to cyber-based attacks. The consequences of a successful cyber attack (that brings operations to a halt) can have a debilitating impact on the United States. For example, if a terrorist organization manages to gain unauthorized computer access to the control systems in an electricity generating facility, they can manipulate the generators and high-voltage transformers to overheat and become inoperable. This will result in a cessation of electricity generation and distribution. Companies that depend on a reliable flow of power will find themselves cutoff. Hospitals, banks, traffic lights, and water sanitation facilities will be unable to function due to the lack of power. The cascading effects of the failure of cyber critical infrastructure in the electricity sector for more than a short period of time will result in a significant loss of economic output, a state of chaos, and even the loss of human life (DHS, 2006).

Supervisory Control and Data Acquisition (SCADA) systems are part of the cyber critical infrastructure used in the bulk-power grid system. SCADA systems are utilized in the electricity sector to manage the generation and distribution of electricity across the bulk-power grid. SCADA systems collect information from remotely located field devices/sensors and use that information to balance supply and demand of electricity across the power grid. SCADA systems in the past were designed without security in mind since they operated in mainly isolated environments (Cyber Security Industry Alliance [CSIA], 2008). However, with the adoption of the Internet SCADA systems have succumbed to evolving business pressures. In an effort to become more efficient and productive

SCADA systems have converted to common technologies such as Windows and LINUX operating systems and Web technologies such as TCP/IP. Additionally, many SCADA systems are taking advantage of interconnected environments (CSIA, 2008). Unfortunately, these changes have made SCADA systems vulnerable to cyber attacks and malware.

According to the report *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems*, attacks on control systems (i.e., SCADA) are increasing (Byres & Lowe, 2004). According to this report 70% of cyber attacks originate from an exterior source. This 70% is further subdivided into the following sections:

- 36% Internet
- 20% Dial-up Modem
- 12% Remote Access – unknown
- 8 % Virtual Private Networks
- 8% Wireless
- 8% Telco
- 4% SCADA
- 4% Trusted 3rd Party Connection

The consequences of successful cyber attacks are monetary losses of over a million dollars (50% of the cases) and loss of control of the physical facilities (29% of cases). This report also stated cyber attacks were under reported by a ration of 1 to 10 (Byres & Lowe, 2004). The under reporting is indicative of the lack of understanding of the significance of the threat and not being aware of the increasing prevalence of cyber attacks. This is confirmed by the *E-Crime Survey* conducted in 2007.

The E-Crime Survey shows a 12% increase in electronic crime was experienced along with a 5% decrease in information technology security spending. The electricity sector represented 2% of the respondents in this survey. This survey also noted that many electronic crimes were not reported due to negative publicity (22%) and due to the fear that competitors would use

that information to their advantage (13%) (CSO Magazine, U.S. Secret Service, CERT Program, & Microsoft Corporation, 2007).

Cyber attackers are aware of this situation and are actively attacking attractive targets. The bulk-power grid system is one of these attractive targets, since it provides the electricity needed by other critical infrastructures to function. According to Tom Donahue, a senior Central Intelligence Agency analyst, the electricity sector has been a target of cyber attacks launched through Internet connections. This disclosure was presented at a conference on SCADA security hosted by SANS Institute in 2008 (Donahue, 2008).

Since the private sector owns the majority (85%) of the electric critical infrastructure in the United States it is imperative for the government and the private sector to work together in securing the cyber critical infrastructure of the bulk-power grid system (Office of Homeland Security [OHS], 2002). It is important to understand the efforts made to date, since these past efforts will provide insight into future successes and failures to secure the cyber critical infrastructure of the bulk power grid system.

2.2. Public and Private Sectors Participants

The main participants involved in securing cyber critical infrastructure for the bulk-power grid system fall into two categories: the private sector and the public sector. The private sector consists of owners and operators of the power grid system and they are represented by NERC. The public sector consists of DHS, DOE, and FERC.

NERC provides direction to the electricity sector in regards to improving the reliability of the bulk-power grid system. NERC encouraged the adoption of reliability measures by providing plans, guidelines, standards, training, and education. NERC's reliability measures were voluntary until 2005. A major blackout in 2003 resulted in FERC empowering NERC to develop and enforce reliability standards (North American Electric Reliability Corporation [NERC], 2008f).

DHS, DOE, FERC, and GAO represent the public sector. DHS' role is to supervise critical infrastructure protection efforts. DOE's role is a coordinating function between DHS and the private sector. FERC's role is regulatory, creating legislation when it is required. In general, regulations are the last option pursued in critical infrastructure protection efforts. The GAO provides progress and evaluation reports on governmental activities.

2.3. Making Sense of all the Developments

The public and private sectors have contributed to many cyber critical infrastructure protection developments over the last eleven years. It is difficult to make sense of the numerous developments that have occurred. There is a need to compile and organize the key developments that have contributed to cyber critical infrastructure protection in the electricity sector, to help provide perspective on what has been accomplished and what remains to be done. That is what this research attempts to accomplish.

CHAPTER 3. METHODOLOGY

3.1. Identifying Documents on Developments

Background information from the literature review shows that the key participating organizations involved in protection efforts to secure the bulk-power-grid are: DHS, DOE, NERC, and FERC. The Web sites of these organizations are searched by keywords to find documents on developments in cyber critical infrastructure protection. These queries included the following keywords and phrases:

- Critical infrastructure
- Critical infrastructure protection
- Cyber critical infrastructure
- Cyber critical infrastructure protection
- Power grid
- Cyber security
- Cyber vulnerabilities
- Reliability standards
- Power outages
- SCADA

The documents identified by the queries were examined to determine if multiple players contributed to the effort – signifying a coordinated effort. Developments that had multiple contributors were selected to be included in this research report.

Additionally, developments that have been identified in the news as key events that resulted in progress in cyber critical infrastructure protection were

included. These are major legislation developments which were listed on the Web sites of these organizations.

3.2. Processing of Documents

The documents retrieved were processed following these steps:

1. Developments were put in temporal order to provide a timeline for cyber protection efforts regarding the bulk-power grid system.
2. Developments were then grouped into DHS (including DOE), NERC, and FERC categories.
    a. The developments were then analyzed to determine what earlier developments contributed to later developments.
    b. Developments were analyzed for trends and findings and compared with GAO progress reports.
3. Then the final conclusion(s) of this research is presented.

CHAPTER 4. RESULTS

4.1. Key Developments Involving Cyber Critical Infrastructure

There are several key developments that have shaped the course of cyber critical infrastructure protection measures for the bulk-power grid system. The developments are classified by year and range from 1997 to 2008. Table 1 shows the 23 developments included in this report.

These key developments involving cyber critical infrastructure protection are divided into three groups. The groups are DHS (included DOE), NERC, and FERC. The key developments are partitioned into the group they are associated with. Each development is then analyzed by the following: what it is, why it is important, and its results. A summary of each group is provided at the end of the group section.

Table 1 Key Developments from 1997- 2008

Ref No.	Year	Development
1	1997	Critical Foundations Report
2	1998	Presidential Decision Directive 63
3	1998	NERC as Coordinator for the Electricity Sector
4	2000	Electricity Sector ISAC
5	2002	NERC's Security Guidelines
6	2002	National Strategy for Homeland Security
7	2002	Homeland Security Act
8	2003	Critical Energy Infrastructure Information Rule
9	2003	The National Strategy to Secure Cyberspace
10	2003	Urgent Action – 1200 Cyber Security Standards
11	2003	Reliability Standards Process Manual
12	2003	Northeast Blackout
13	2003	Homeland Security Presidential Directive 7
14	2004	Protected Critical Infrastructure Information Program
15	2005	Energy Policy Act
16	2006	Electricity Reliability Organization
17	2006	Reliability Standards Development Procedures
18	2006	National Infrastructure Protection Plan
19	2006	Reliability Standards on Critical Infrastructure Protection
20	2006	Roadmap to Secure Control Systems in the Energy Sector
21	2007	Reliability Standards Development Plan: 2008-2010
22	2007	Energy Critical Infrastructure & Key Resources Sector-Specific Plan
23	2008	Mandatory Reliability Standards for Critical Infrastructure Protection

4.2. The Three Divisions

4.2.1. DHS Developments

The developments under DHS consist mostly of plans for securing critical infrastructure. All the plans address issues and vulnerabilities created by the utilization of information technology (common off-the-shelf technology) used in

critical infrastructure in an interconnected, networked environment. These environments in the electricity sector commonly employ SCADA systems. These SCADA systems are vulnerable to cyber attacks that accompany the networked environment of information technology products. Since 85% of the electricity sector's critical infrastructure is privately owned (OHS, 2002), all plans emphasize the public-private partnership efforts to share information so vulnerabilities can be identified, threats can be assessed, and mitigation plans and solutions can be developed and implemented. Each plan builds upon the previous plans. Figure 1 shows what developments contributed to each resulting development. The figure presents a visual guide to the relationships between the developments.

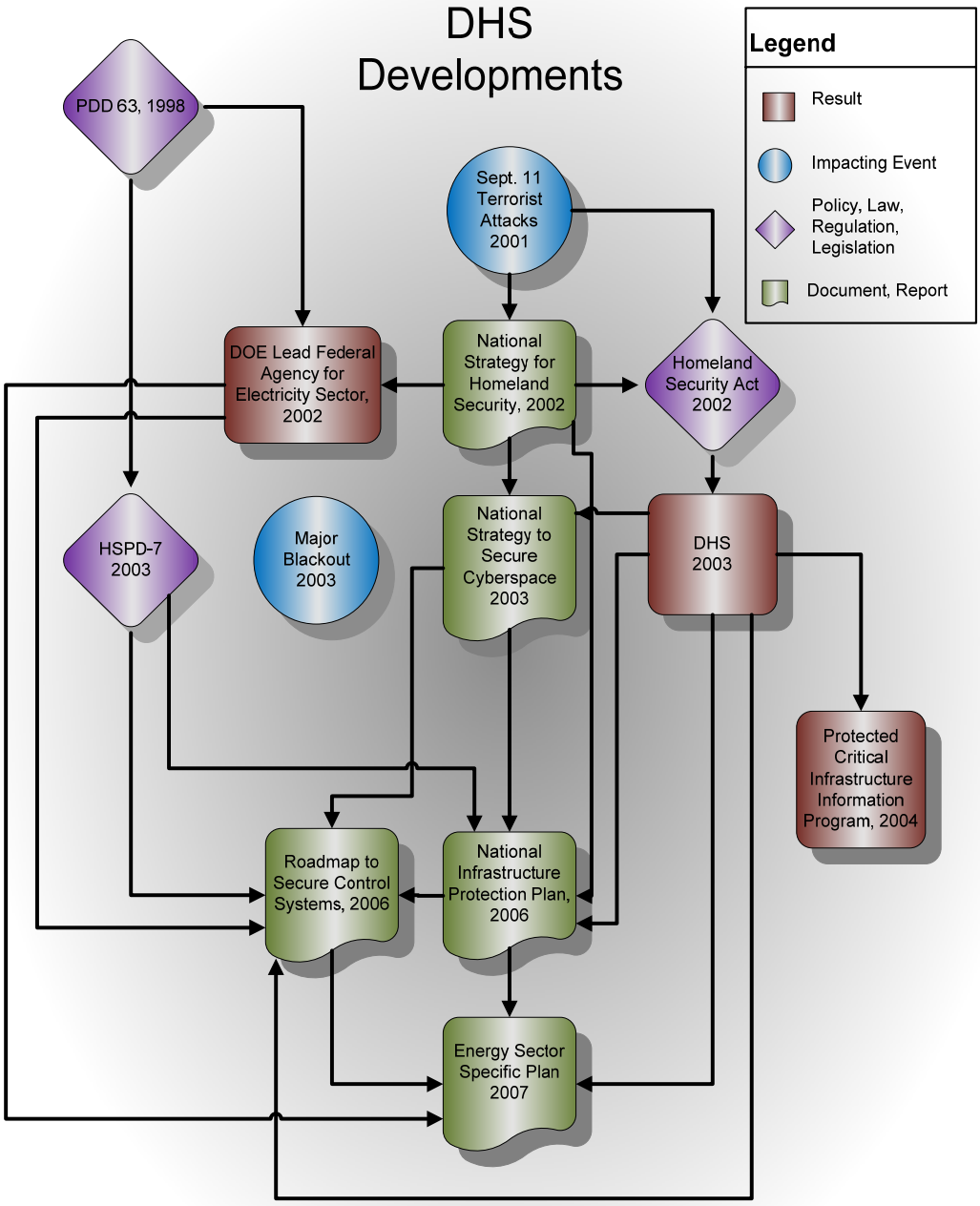

Figure 1 DHS Developments

4.2.1.1. Presidential Decision Directive 63

4.2.1.1.1. What it is

Presidential Decision Directive 63 (PDD 63) was the result of the *Critical Foundations* report in 1998. PDD 63 discusses federal involvement in critical infrastructure protection to assist in the elimination of any significant physical and cyber threats to critical infrastructure (The White House, 1998).

4.2.1.1.2. Why is it important

This directive set a goal of reaching the state of critical infrastructure assurance by 2003. This state of assurance means the following: “Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States” (The White House, 1998, p. 3). The directive orders each sector to start working on plans to secure critical infrastructure, especially cyber critical infrastructure (The White House, 1998).

4.2.1.1.3. Results

As a result of this directive DOE was named the lead agency of the electricity sector (The White House, 1998). This directive brought attention to the need to secure critical infrastructure. However the goal of reaching the state of critical infrastructure assurance was not reached in 2003. This was proven by a major power outage in the Northeastern United States in 2003.

4.2.1.2. National Strategy for Homeland Security

4.2.1.2.1. What it is

The Office of Homeland Security created the report: *National Strategy for Homeland Security* in 2002. This was the first national strategy developed to aid in the prevention of terrorist attacks, in response to the September 11, 2001 attacks (OHS, 2002).

4.2.1.2.2. Why is it important

The idea of one federal agency leading and overseeing critical infrastructure protection was first introduced in this strategy (OHS, 2002). This

agency became DHS. The *National Strategy for Homeland Security* also set the original goals that DHS was to be involved with (OHS, 2002). These goals are plans for securing cyberspace and infrastructure.

4.2.1.2.3. Results

This strategy resulted in the *National Strategy to Secure Cyberspace* and the *National Infrastructure Protection Plan* (NIPP). The importance of the public-private partnership efforts in securing critical infrastructure is also discussed. Additionally, the concepts of DHS and information sharing (presented in this strategy) were used in the *Homeland Security Act* of 2002.

4.2.1.3. Homeland Security Act of 2002

4.2.1.3.1. What it is

The *Homeland Security Act* of 2002 was a result of the terrorist attacks on September 11, 2001 (OHS, 2002).

4.2.1.3.2. Why is it important

This act shows the intention of the government to become involved in critical infrastructure protection measures. The act authorizes the creation of the Department of Homeland Security (DHS) (HSA, 2002). Section 214 in Title II of the act protects private companies that share their critical infrastructure information with government. The information voluntarily submitted to the government is exempt from disclosure under *Freedom of Information Act* and cannot be used in civil actions (HSA, 2002). Section 214's goal is to encourage private industry to voluntarily share their vulnerability and threat information with the government, by providing the submitting entity relative immunity from litigation.

4.2.1.3.3. Results

From the *Homeland Security Act* of 2002, the DHS was created in 2003. DHS goal is to:

> Build and maintain a complete, current, and accurate assessment of vulnerabilities and preparedness of critical targets across critical

> infrastructure sectors. The Department would thus have a crucial capability that does not exist in our government today: the ability to continuously evaluate threat information against our current vulnerabilities, inform the President, issue warnings, and effect action accordingly. (p. 33)

In order to accomplish this goal, emphasis was put on developing public-private partnership and encouraging the sharing of critical infrastructure information (such as vulnerabilities) with the government.

4.2.1.4. The National Strategy to Secure Cyberspace

4.2.1.4.1. What it is

DHS published *The National Strategy to Secure Cyberspace* in 2003. In this strategy the DHS is responsible for leading the efforts to protect critical infrastructures from cyber attacks (The White House, 2003a).

4.2.1.4.2. Why is it important

DHS defines its responsibilities in this strategy (The White House, 2003a):

1. Developing a plan to implement a strategy of threat and vulnerability reduction
2. Security awareness and training
3. Securing government cyberspace
4. Cyberspace security response program

This strategy also addresses the security issues with SCADA systems in the electricity sector. SCADA systems are computer based systems that remotely control the physical processes in the power grid, such as balancing electric load on the grid and increasing electricity generation. SCADA systems are increasing using the Internet to transmit data rather than closed, proprietary networks (The White House, 2003a). DHS works with private sector and DOE to raise awareness of the security issues affecting the commonly used SCADA systems and to promote SCADA security. Some goals for SCADA in *The National Strategy to Secure Cyberspace* are (The White House, 2003a):

1. Work on intrusion detection methods

2. Internet infrastructure security
3. Application security
4. Transmission security (encryption and authentication)

These goals all need to be implemented in an environment that requires real-time responses.

4.2.1.4.3. Results

DHS shows effort by writing down commitments. The strategy also discusses cyber security for SCADA systems. This brings attention to the need to secure cyber critical assets from cyber attacks. In order to accomplish the goals presented in this strategy collaboration and cooperation is needed in the public-private partnership efforts, especially in the area of information sharing to identify issues, establish baselines, and prioritize efforts.

The National Strategy to Secure Cyberspace also resulted in the *National Infrastructure Protection Plan* and the *Roadmap to Secure Control Systems in the Energy Sector* (report). These efforts build upon the concepts presented in *The National Strategy to Secure Cyberspace* and show progress in developing more specific plans.

4.2.1.5. Homeland Security Presidential Directive 7

4.2.1.5.1. What it is

Homeland Security Presidential Directive 7 (HSPD-7) replaced PDD 63 in 2003. HSPD-7 updated the policies presented in PDD 63. This directive requires federal government to be involved in ensuring the continued, reliable functions of critical infrastructure services (The White House, 2003b).

4.2.1.5.2. Why is it important

It also requires a national plan for critical infrastructure be created by 2004, with goals and milestones. DHS is the leading federal agency identified in the directive. Additionally, sector-specific agencies (i.e., DOE) need to report to DHS on an annual basis on progress on critical infrastructure protection within their sector (i.e., electricity sector) (The White House, 2003b).

4.2.1.5.3. Results

HSPD-7 broadened DHS' role by analyzing information, issuing warnings, sharing information, reducing vulnerabilities, mitigating damages, and aiding in recovery efforts (The White House, 2003b). HSPD-7 also called for the NIPP plan to be done in 2004, which was not finally completed until 2006.

4.2.1.6. Protected Critical Infrastructure Information Program

4.2.1.6.1. What it is

In 2004 DHS created the Protected Critical Infrastructure Information Program (PCII Program). This Program enables the private sector to voluntarily submit vulnerabilities and threat information to the DHS on critical infrastructure. DHS in return will analyze the submitted information and determines if it qualifies for protective status from the *Freedom of Information Act*, civil lawsuits and public viewing (DHS, 2007).

4.2.1.6.2. Why is it important

The PCII Program was meant as an incentive to the private sector to share information with the government. The PCII Program is important because the information provided allows the DHS to identify and analyze vulnerabilities to cyber critical infrastructure.

4.2.1.6.3. Results

This program is not being used that much due to concerns over DHS' implementation of it. The electric sector reported in 2005 that they had not used the program since it required paper submission, but probably would when the process went electronic (Poulsen, 2005). In March 2008, the PCII Program did have electronic submission capabilities, however, the digital certificate on the Web site had expired in 2007 (Figure 2).

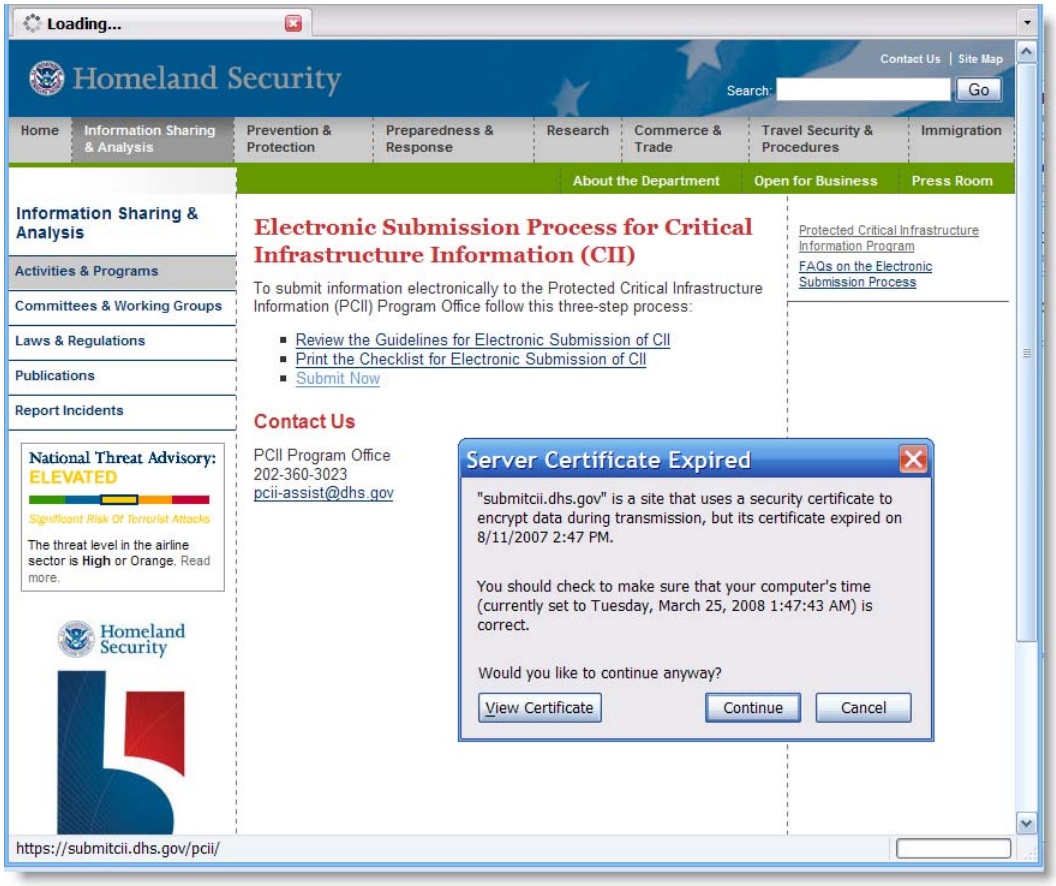

Figure 2 PCII Program Website Certificate

This implies that DHS is experiencing organizational and implementation difficulties.

4.2.1.7. National Infrastructure Protection Plan

4.2.1.7.1. What it is

DHS produced the *National Infrastructure Protection Plan* (NIPP) in 2006 fulfilling the national plan requirement set out in HSPD-7. NIPP confirms DHS' administrative role in critical infrastructure protection activities. The plan requires for each sector agency (i.e., DOE) to submit a sector-specific plan to DHS for securing critical infrastructure within their associated sector (DHS, 2006a).

4.2.1.7.2. Why is it important

Since cyber critical infrastructure runs the physical critical infrastructure in the electricity sector, particular attention was paid to securing cyber assets (e.g., SCADA systems), systems, and networks in the NIPP plan. In order to address the cyber infrastructure issues of SCADA, DHS has created the Control Systems Cyber Security Program, Standards and Best Practices Programs with National Institute of Standards and Technology, Software Assurance Program, a National Vulnerability Database, and the National Cyber Response Coordination Group (DHS, 2006a).

The degree of success of the NIPP depends on convincing the private sector to voluntarily take an active role in the public-private partnership efforts. Some of the main points listed to create value for the private sector to increase information sharing are the following (DHS, 2006a):

1. Provide useful, timely information to private sector
2. Engage private sector in developing policies
3. Proving business benefits to securing critical infrastructure
4. Create an environment that makes adopting security practices attractive to private sector entities
5. Provide support for research into future critical infrastructure protection
6. Conduct interdependencies research
7. Provide recovery support in the event of an incident

4.2.1.7.3. Results

NIPP built upon HSPD-7, *The National Strategy to Secure Cyberspace*, and the *National Strategy for Homeland Security*.

4.2.1.8. Roadmap to Secure Control Systems in the Energy Sector

4.2.1.8.1. What it is

In 2006 DHS and DOE created the *Roadmap to Secure Control System in the Energy Sector* (Roadmap Report). This Roadmap Report establishes a ten

year timeframe to meet its goals. The goals are to assess security, develop protective measures, detect intrusions, and to apply security improvements (DHS & DOE, 2006). The plan stresses the importance of the public-private partnership efforts in achieving this goal.

4.2.1.8.2. Why is it important

The Roadmap Report was a collaborative effort between DOE, DHS, NERC, and private entities within the electricity sector. The Roadmap Report was the result of HSPD-7, *The National Strategy to Secure Cyberspace*, and the NIPP (GAO, 2007a). The report stresses the importance of government (i.e., DHS), industry organizations (i.e., NERC), researchers (i.e., NIST & universities), commercial entities (i.e., vendors), and owners/operators all working together (DHS & DOE, 2006).

The electricity sector relies on SCADA systems to monitor and control electricity generation and transmission in the bulk-power grid system. According to the Roadmap Report "over half of the 3,200 power utilities are estimated to have some form of SCADA system" employed (DHS & DOE, 2006, p. 8). This report also noted that legacy SCADA systems were designed without secure password policies and with limited to no data protections mechanisms. Also applying security to legacy SCADA systems is expensive and without a well known example of a cyber attack to a SCADA system in the electricity sector, the business case is difficult to justify (DHS & DOE, 2006).

Some of the key obstacles to achieving the goals listed in the Roadmap Report are the following (DHS & DOE, 2006):

- Required employee clearance levels to access classified critical infrastructure information
- Establishing a business case to encourage control systems security
- Lack of government funding
- Working with many federal offices instead of just one
- Concern over how protected is submitted critical infrastructure information

- Vendor buy-in to solutions

4.2.1.8.3. Results

The Roadmap Report was the result of effective public-private partnership efforts. It identified obstacles and set a timeframe for securing SCADA systems. It built upon previous plans.

4.2.1.9. Energy Critical Infrastructure and Key Resources Sector-Specific Plan

4.2.1.9.1. What it is

Energy Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (Redacted) is referred to as the Sector-Specific Plan. The Sector-Specific Plan involves employing a risk management framework to reach it cyber security goals. There are four main goals presented in the plan (DHS & DOE, 2007):

1. Information sharing and communication to establish awareness
2. Physical and cyber security implemented by employing risk management principles
3. Coordination and planning where roles are clearly defined, interdependencies are understood, and exercise conducted
4. Gaining public confidence

4.2.1.9.2. Why is it important

To reach the goal of cyber critical infrastructure protection the application of risk management methodology is employed in this plan as required by NIPP. The Sector-Specific Plan states “Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resiliency” (DHS & DOE, 2007, p. 2). The risk management framework involves six reiterative steps: (1) set goals, (2) identify assets, (3) assess risks, (4) prioritize security programs, (5) implement security programs, and (6) measure effectiveness (DHS & DOE, 2007). See Figure 3 for DHS’s risk management framework. The performance metrics used to track critical

infrastructure progress are qualitative and quantitative in nature and are still being developed by DHS and the electricity sector (DHS & DOE, 2007).

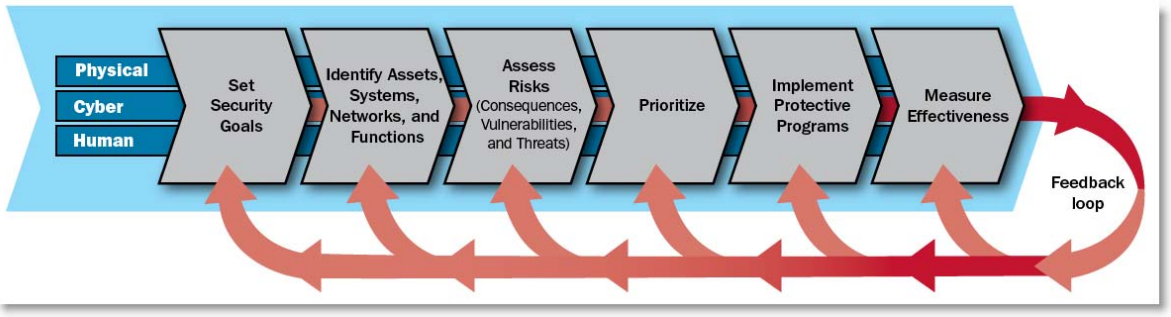

Figure 3 DHS's Risk Management Framework (DHS & DOE, 2007, p. 6)

4.2.1.9.3. Results

One of the most valuable outcomes from this plan is the increased communication and the development of trusted relationships between the government and the private electricity sector entities (DHS & DOE, 2007). This plan fulfills the sector specific plan called for by NIPP. The Sector-Specific Pan also built off the Roadmap Report. This was also a collaborative effort between DHS, DOE, and NERC (DHS & DOE, 2007).

4.2.1.10. DHS Summary

The September 11th attacks in 2001 brought attention to the disorganized government response to a terrorist attack on the homeland (National Commission on Terrorist Attacks, 2004). DHS was created as a response to these attacks. One of DHS main responsibilities is to be the focal point of critical infrastructure protection efforts. As the focal point, DHS is tasked with developing and implementing strategies and plans on critical infrastructure protection. These plans appear to build off each other; however on closer examination there is a lot of repetition. DHS has identified and brought attention to the vulnerabilities of

SCADA systems in these plans and strategies. DHS falls short in implementing the plans, due dates have been missed and effective processes for information sharing with the private sector are still not in place.

4.2.2. NERC Developments

The developments under NERC can be considered mainly instructional in nature. These developments consist mostly of creating guidelines and standards to achieve a level of sustained reliability in the bulk-power grid system. Each standard development process builds on previous processes developed by NERC. Due to the threats to SCADA systems in the electricity sector, specific attention is paid to cyber critical infrastructure standards development. Additionally since the government put such emphasis on information sharing NERC did put some effort into this area. Figure 4 shows what developments contributed to each resulting standards development. The figure presents a visual guide to the evolution of standards over the time period.

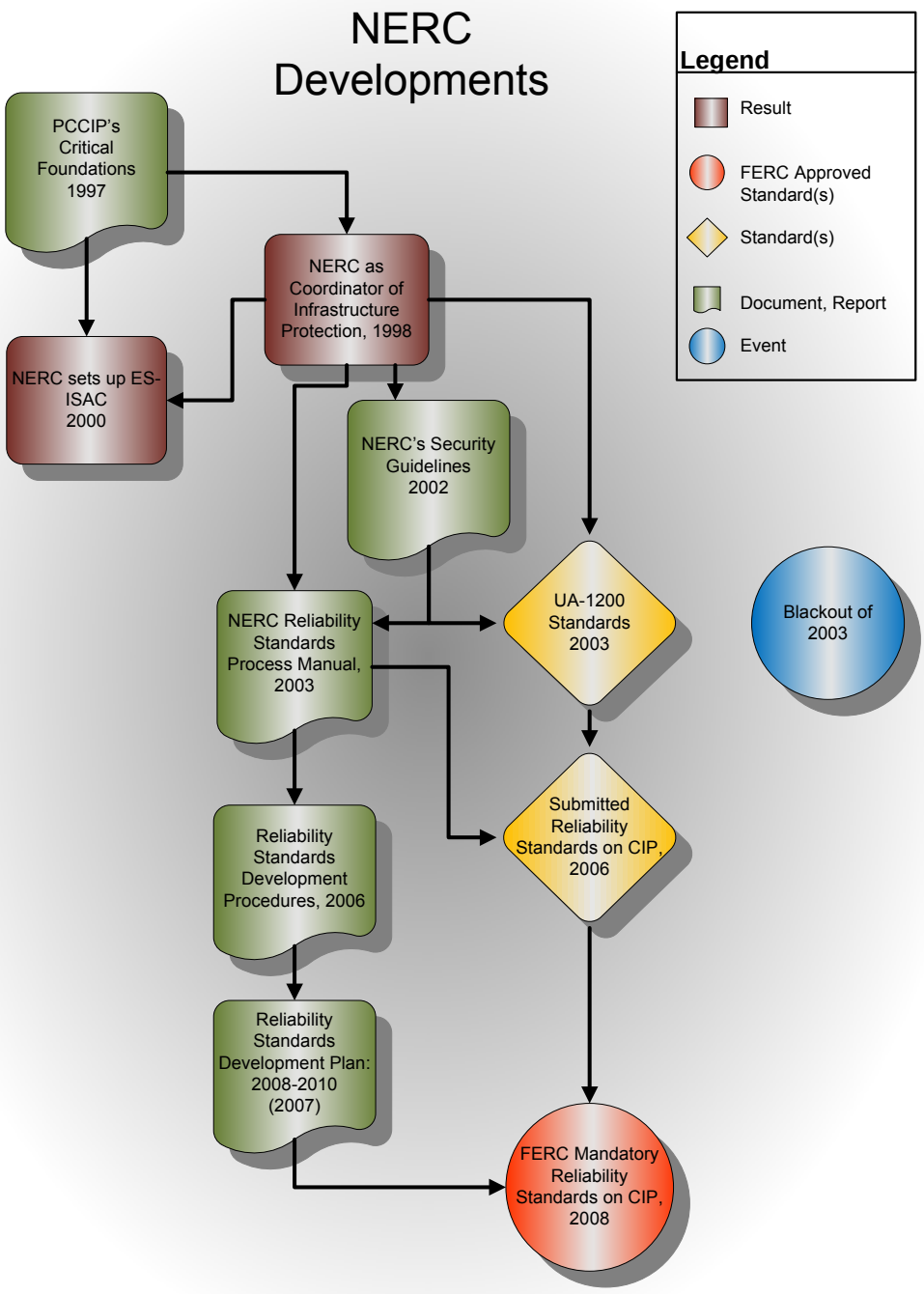

Figure 4 NERC Developments

4.2.2.1. Critical Foundations

4.2.2.1.1. What it is

The *Critical Foundations* report was produced by the President's Commission on Critical Infrastructure Protection in 1997 and it reports on the perceived threats to critical infrastructure and the proposed solutions (PCCIP, 1997).

4.2.2.1.2. Why is it Important

The report discusses the integration of connected computer systems, telecommunications, and infrastructures which have produced a complex web of interdependencies. This environment is vulnerable to cyber-based attacks. This report brought attention to the need for critical infrastructure protection measures.

The *Critical Foundations* report also identified NERC as a model for partnership success (PCCIP, 1997).NERC had a long history of successfully working with the Federal Bureau of Investigations and the DOE in sharing information (Costantini, 2002). Building on this concept of information sharing, the report recommended the development of repositories where information could be stored, accessed, and shared by the private sector and the public sector. These repositories were identified as Information Sharing and Analysis Centers (ISACs) (PCCIP, 1997).

4.2.2.1.3. Results

The proposed solutions of this report laid the groundwork for future plans, strategies, legislation, and reliability standards. The top recommendation from the *Critical Foundations* report was that information sharing was vital in protecting critical infrastructure.

In 1998, The DOE approached NERC and asked them to take on the role of Coordinator for Critical Infrastructure Protection for the electricity sector and also to set up the ISAC.

4.2.2.2. NERC as Coordinator for Electricity Sector

4.2.2.2.1. What it is

NERC became the Coordinator of the Electricity Sector in 1998. As the Coordinator of Critical Infrastructure Protection in the electricity sector, NERC is responsible for (NERC, 2002b):

- Assessing bulk-power system vulnerabilities
- Developing plans to mitigate these vulnerabilities
- Developing programs to identify and prevent attacks
- Developing plans for sharing information on attacks currently in progress
- Developing plans to recover from attacks

4.2.2.2.2. Why is it Important

NERC becomes the focal point for organizing and monitoring cyber critical infrastructure protection efforts in the electricity sector.

4.2.2.2.3. Results

From this role, NERC created plans, processes, procedures and standards to secure the bulk-power grid.

4.2.2.3. Electricity Sector Information Sharing and Analysis Center

4.2.2.3.1. What it is

In 2000 NERC established the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The ES-ISAC's function is to facilitate the sharing of information between the public and private sectors, to analyze sector interdependencies, and participate in infrastructure exercises (Leffler, 2002).

4.2.2.3.2. Why is it Important

The ES-ISAC collects and disseminates information relating to threats and vulnerabilities (both cyber and physical) relating to the bulk-power grid system. It shares information with DHS and private entities within the electricity sector.

4.2.2.3.3. Results

This is one way to share information with the government. However, it is questionable how much it is used as a vehicle for information sharing.

4.2.2.4. Security Guidelines for the Electricity Sector

4.2.2.4.1. What it is

In 2002, NERC produced the *Security Guidelines for the Electricity Sector*. These are general guidelines for protecting electric critical infrastructure systems and are advisory in nature. These guidelines consist of the following (NERC, 2002c):

1. Vulnerability & Risk Assessments
2. Threat Response Capabilities
3. Emergency Management
4. Continuity of Business Processes
5. Communications
6. Physical Security
7. Information Technology/Cyber Security
8. Employment Screening
9. Protect Sensitive Information

The section on information technology and cyber security discusses implementing a risk management program which has been proven extensively in other industries, as an effective way to identify and assess risk. The section also discussed implementing cyber access controls involving authorization, authentication, and monitoring. Cyber intrusion detection tools and firewall technology products were also briefly discussed (NERC, 2002c).

4.2.2.4.2. Why is it Important

The cyber security guideline warns about giving enough attention to securing Energy Management System, SCADA systems, and operating systems. These technologies should employ security measures such as access control. Access control should involve authentication of user by smart cards, bio-metrics,

and or passwords. Access control should provide monitoring to establish an audit trail (date and time of user authentication, user initiated events, etc.) (NERC, 2002b).

4.2.2.4.3. Results

NERC took on the responsibility of developing reliability standards for electricity generation and transmission. These guidelines provided a foundation that other developments built upon. These security guidelines were applied in the *Reliability Standards on Critical Infrastructure Protection*.

4.2.2.5. Urgent Action – 1200 Cyber Security Standard

4.2.2.5.1. What it is

The purpose of NERC's *Urgent Action – 1200 Cyber Security Standards* (UA-1200) is to protect cyber critical infrastructure in the bulk-power grid system. These standards were developed in 2003. The UA-1200 consists of sixteen sections relating to cyber security protection measures (Table 2) (NERC, 2003c).

Table 2 UA-1200 Cyber Security Standards for the Electricity Sector

No.	Standard Name	Description
1201	Cyber Security Policy	Have a written policy in effect
1202	Critical Cyber Assets	Identify critical cyber assets
1203	Electronic Security Perimeter	Identify all interconnected cyber assets, all points of electronic entry
1204	Electronic Access Controls	Identify access controls and implementation within the electronic security perimeter(s)
1205	Physical Security Perimeter	Identify the physical perimeter that contains all access points and cyber assets
1206	Physical Access Controls	Identify access controls for physical security perimeter
1207	Personnel	List of personnel granted access to cyber assets and access rights
1208	Monitoring Physical Access	Identify tools and procedures for monitoring physical access
1209	Monitoring Electronic Access	Identify tools and procedures for electronic physical access
1210	Information Protection	Identify access restrictions to sensitive information
1211	Training	Shall address 1201, 1204, 1206, 1210, 1214
1212	Systems Management	Identify policies and procedures
1213	Test Procedures	Identify test and acceptance criteria for adding, modifying cyber assets
1214	Electronic Incident Response Actions	Identify what to do in event of electronic incident
1215	Physical Incident Response Actions	Identify what to do in event of physical incident
1216	Recovery Plans	Define plans, procedures for recovery after an incident

4.2.2.5.2. Why is it Important

The UA-1200 was meant as a temporary, stop-gap measure and can be considered a primer for later efforts in cyber security standards. It was the first attempt to create standards for cyber critical infrastructure for the bulk-power grid system (NERC, 2003c). These measures span having a written cyber security

policy to recovery plans. If applied correctly the UA-1200 provide a certain level of cyber critical infrastructure protection. The UA-1200 was to be in effect for only one year or until it is replaced by permanent standards (NERC, 2003c).

4.2.2.5.3. Results

These standards later developed into the *Reliability Standards on Critical Infrastructure Protection*.

4.2.2.6. Reliability Standards Process Manual

4.2.2.6.1. What it is

The NERC's *Reliability Standards Process Manual* is a step-by-step process for creating, changing, and deleting standards (NERC, 2003a). These reliability standards must contain the following elements (NERC, 2003a):

- Identification number
- Title
- Effective date and status
- Purpose and requirements
- Measurements
- Expected performance
- Compliance monitoring process

The process of developing a standard involves these main steps:

1. Request to develop standard (sent to Standard Authorization Committee)
2. Proposed standard is posted for public comment
3. Solicitation survey to generate consensus on development process
4. Standard is drafted
5. Solicit public comments on the draft standard
6. Field testing
7. Analysis of field tests and comments
8. Draft standard is voted on

9. Standard is either adopted or rejected
10. Implementation of standard

4.2.2.6.2. Why is it Important

This standards development process provides continuity. This process is also accredited by American National Standards Institute in March of 2003, giving the process validity (NERC, 2003a).

4.2.2.6.3. Results

This process was used in the development of *Reliability Standards on Critical Infrastructure Protection*. This process manual later developed into the *Reliability Standards Development Procedures* in 2006. The changes in the *Reliability Standards Development Procedures* from the process manual have to do with FERC's order certifying NERC as the ERO (NERC, 2006j).

4.2.2.7. Reliability Standards on Critical Infrastructure Protection

4.2.2.7.1. What it is

In 2006 NERC replaced the UA-1200 with the *Reliability Standards on Critical Infrastructure Protection*. These eight standards deal with securing cyber critical infrastructure of the bulk-power grid system from cyber attacks (FERC, 2008a). The *Reliability Standards for Critical Infrastructure Protection* is referred to as: CIP-002-1 to CIP-009-1 (Table 3) (FERC, 2008a).

Table 3 Reliability Standards for Critical Infrastructure Protection

Standard	Description
CIP-002-1	Cyber Security — Critical Cyber Asset Identification
CIP-003-1	Cyber Security — Security Management Controls
CIP-004-1	Cyber Security — Personnel & Training
CIP-005-1	Cyber Security — Electronic Security Perimeter(s)
CIP-006-1	Cyber Security — Physical Security of Critical Cyber Assets
CIP-007-1	Cyber Security — Systems Security Management
CIP-008-1	Cyber Security — Incident Reporting and Response Planning
CIP-009-1	Cyber Security — Recovery Plans for Critical Cyber Assets

4.2.2.7.2. Why is it Important

NERC submitted the *Reliability Standards on Critical Infrastructure Protection* to FERC for approval. These standards are a comprehensive set that when implemented correctly should provide bulk-power grid reliability (FERC, 2008a). Each standard is meant to build on top of each other; they should be implemented in order. They incorporate a risk-based approach for implementation. These standards apply to the following entities in the electricity sector (FERC, 2008a):

- Reliability coordinators
- Balancing authorities
- Interchange authorities
- Transmission service providers
- Transmission owners
- Transmission operators
- Generator owners
- Generator operators
- Load serving entities
- NERC

- Regional Reliability Organizations

These entities are allowed to self-certify on a semi-annual basis until compliance due dates are reached. There is a three-year phased in timeframe for compliance. Entities should be ready for external audit compliance tests by 2010 (FERC, 2008a).

4.2.2.7.3. Results

These standards incorporated UA-1200 and followed the development process outlined in NERC's *Reliability Standards Process Manual*. These standards are called the *Mandatory Reliability Standards on Critical Infrastructure Protection* after they were approved by FERC in 2008 (FERC, 2008a).

4.2.2.8. Reliability Standards Development Plan: 2008-2010

4.2.2.8.1. What it is

The *Reliability Standards Development Plan: 2008-2010* was created by NERC in 2007. This plan is a management tool to guide development in reliability standards (a work plan) (NERC, 2007e). This plan is dynamic; it changes over time based on priorities and what has been accomplished.

4.2.2.8.2. Why is it Important

In this plan the cyber security reliability standards project is scheduled to start in 2009. The standards are tested to meet the following ten objectives (NERC, 2007e):

1. Applicability
2. Purpose
3. Performance requirements
4. Measurability
5. Technical basis in engineering and operations
6. Completeness
7. Consequence for noncompliance,
8. Clear language

9. Practicality
10. Consistent terminology

This plan changes the completion date on cyber critical infrastructure protection until the second quarter 2011 (NERC, 2007e).

4.2.2.8.3. Results

The cyber security project is delayed by one year. Originally the electricity sector was supposed to be 100% audit compliant by the end of 2010. This plan incorporates parts from the *Reliability Standards Development Procedures* and is being used to implement the *Mandatory Reliability Standards on Critical Infrastructure Protection.*

4.2.2.9. NERC Summary

Developments involving NERC show continuous work on creating comprehensive guidelines and standards. The establishment of official manuals and procedures for designing and approving standards for cyber critical infrastructure insure that specific requirements are met before the standard is passed. The process of creating, changing, or removing a standard is approved by the National Institute of Standards and Technology, giving the process recognized validation. The process of sending the proposed standard out for comments to the entities in the electricity sector and the final ballot voting on the proposed standard, creates a collaborative environment and promotes industry buy-in. For example, the draft of the UA-1200 cyber security standard was posted for comment and got around 700 responses (NERC, 2005). However, obstacles still persisted in the adoption of these voluntary standards by the electricity sector. This became clear after the 2003 Northeast Blackout. The investigation showed that voluntary standards were not being adopted (Natural Resources Canada & US Department of Energy, 2006). This resulted in regulations to force entities in the electricity sector to implement standards to achieve reliability in the bulk-power grid system.

4.2.3. FERC Developments

The developments under FERC are all of a regulatory nature. FERC is an independent regulatory agency within the DOE. FERC issues the regulations needed to establish reliability in the bulk-power grid system (FERC, 2007b). The public-private partnership efforts between FERC and NERC are present in all these resulting rules. NERC submits a proposed standard and FERC gives the standard its seal of approval or sends it back to NERC for revisions. NERC in turn can make comments on revisions and FERC considers those comments in its final rule making process. Figure 5 shows the series of regulations affecting cyber critical infrastructures in the electricity sector.

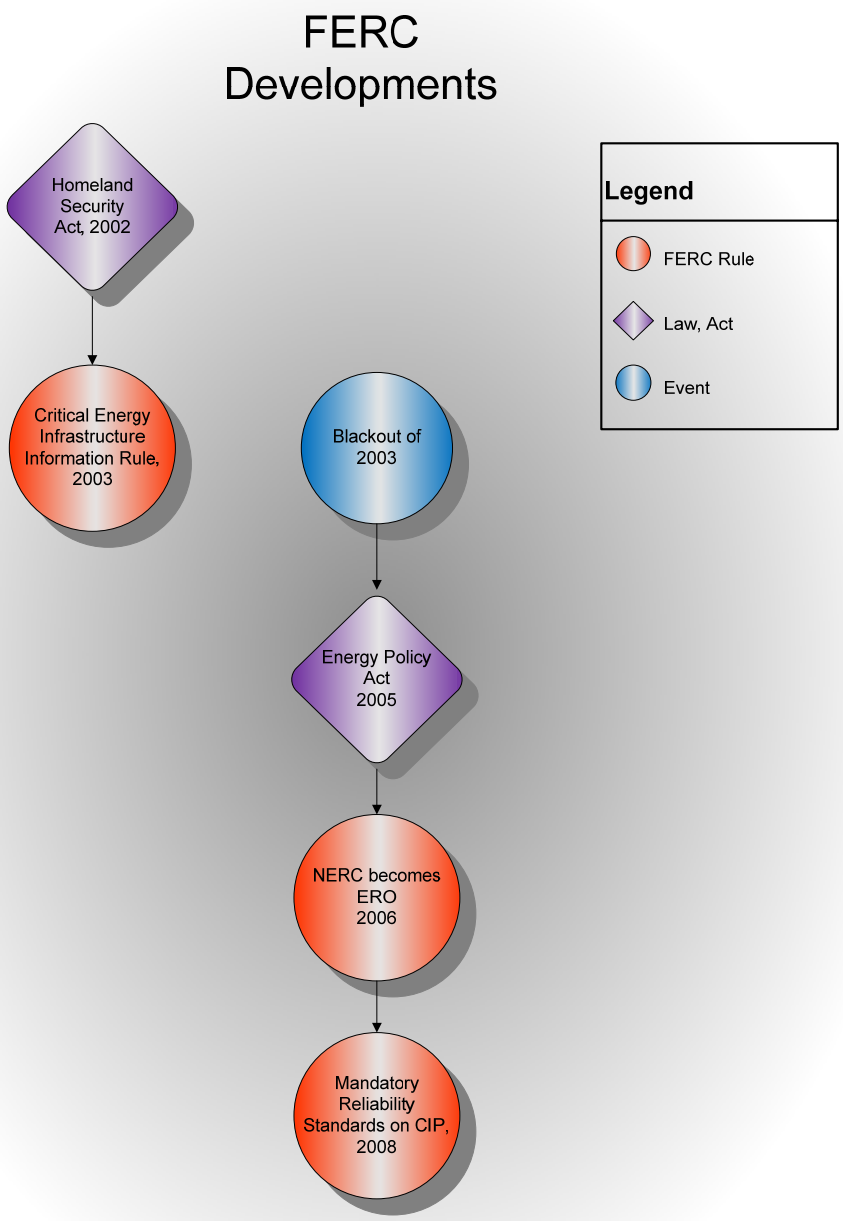

Figure 5 FERC Developments

4.2.3.1. Critical Energy Infrastructure Information Final Rule

4.2.3.1.1. What it is

Critical Energy Infrastructure Information Final Rule (CEII Rule) was issued by FERC and clarifies the process for gaining access to protected information that was voluntarily submitted to DHS from the energy sector. The goal of this Rule is to make it difficult for the public to attain physical or cyber critical infrastructure information (voluntarily submitted to DHS) while making the protected information available to energy market consultants that need it to aid in critical infrastructure protection efforts (FERC, 2003).

4.2.3.1.2. Why is it Important

This Rule is a response to the lack of cyber critical infrastructure information sharing with the government. The electricity sector is concerned about sharing information on power system vulnerabilities, cyber security incidents, and other sensitive information that could be detrimental if that information was to be released into the public realm. Even though the *Homeland Security Act* of 2002 (Title II) addressed protecting critical infrastructure information there is still reluctance to share information with the government. FERC took measures to alleviate concern over this issue by incorporating specific language as to what information is considered protected and who is authorized to access this protected information.

NERC responded to the notice of this impending rule by providing comments to FERC to be considered. A 30 day window was requested to respond to information that was submitted as critical infrastructure information, but did not qualify as it (so submitting entity could take back the information and still retain control over its dispersal).The use of non-disclosure agreements was requested for the released protected information. NERC also wanted relationship interdependencies information on SCADA and Energy Management Systems to be deemed protected information (NERC, 2002a).

4.2.3.1.3. Results

The final rule took into consideration the comments from NERC and from specific entities within the electricity sector. Some of these comments were added to the final rule and some were not.

4.2.3.2. Northeast Blackout of 2003

4.2.3.2.1. What it is

The Northeastern Blackout left 50-million people without power. It occurred on August 14th, 2003. It was the largest blackout experienced in the United States in recent history. 100 power plants failed and 531 generators tripped. This was a cascading power outage. It took 30 hours to restore power (Hilt, 2006). See Figure 6 for the National Oceanic and Atmospheric Administration (NOAA) images of power outage effect before and after.

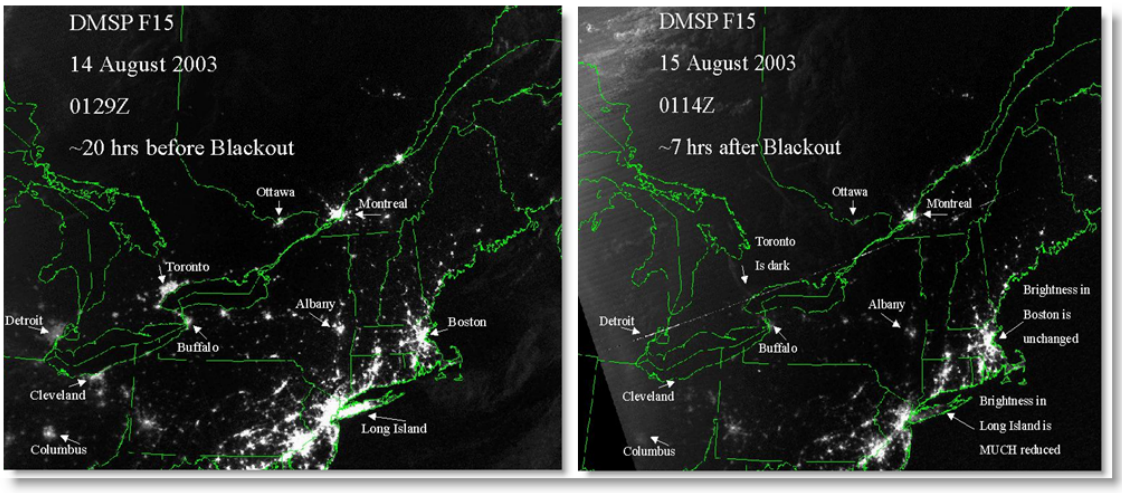

Figure 6 NOAA Northeast Blackout Images Before and After (National Oceanic and Atmospheric Administration, 2003)

4.2.3.2.2. Why is it Important

The Northeast Blackout brought attention to the lack of voluntary compliance to guidelines and standards meant to secure the bulk-power grid system. Questions on whether voluntary standards had been implemented were asked. The findings of the investigation showed that many entities involved in the cascading blackout did not implement the voluntary standards (U.S.-Canada Power System Outage Task Force, 2004). This would be the trigger that led to the development of regulations to enforce compliance in 2005.

4.2.3.2.3. Results

As a result the *Energy Policy Act* of 2005 was passed.

4.2.3.3. Energy Policy Act of 2005

4.2.3.3.1. What it is

The act empowers FERC to certify an Electric Reliability Organization (ERO). The ERO can develop and make compulsory reliability standards for the bulk-power grid system, with the full force of law behind them (can enforce monetary penalties for non-compliance) (Energy Policy Act, 2005). The new section 215 of the *Federal Powers Act* made this possible. This section allows the ERO to develop and enforce reliability standards subject to review by FERC (FERC, 2007).

4.2.3.3.2. Why is it Important

The *Energy Policy Act* solves the problem of non-compliance to reliability standards.

4.2.3.3.3. Results

Since NERC had already shown a track record of developing standards, NERC applied to become the ERO. In 2006 NERC was certified as the ERO. This gave NERC the power needed to enforce critical infrastructure reliability standards on the electricity sector (FERC, 2007). This should result in a certain level of bulk-power grid reliability by the compliance and enforcement of standards.

4.2.3.4. Mandatory Reliability Standards on Critical Infrastructure Protection

4.2.3.4.1. What it is

FERC approved NERC's cyber security standards in 2008 as the *Mandatory Reliability Standards on Critical Infrastructure Protection* (FERC, 2008a) (See Appendix A for details on CIP- 002 through CIP-009 standards).

4.2.3.4.2. Why is it Important

Entities in the electricity sector must comply with the standards or face monetary fines of up to one-million dollars per day (GAO, 2007a). There are 3,284 electric utility companies in the United States in 2005 and 3,029 are considered small utilities under the definitions of the Small Business Administration. Under the requirements of NERC there are 1,000 entities that will be required to comply with the *Mandatory Reliability Standards on Critical Infrastructure Protection*. Of these – 632 are small entities (FERC, 2008a). Entities who must comply are defined as those entities that can material effect the functioning of the bulk-power grid system. They also include the entities described in Section 4.2.2.7.2.

4.2.3.4.3. Results

Mandatory Reliability Standards on Critical Infrastructure Protection does not address how to measure progress in reaching compliance. All required entities must be compliant by 2011. The dates for compliance were determined by NERC with input from the entities within the electricity sector (FERC, 2008a). At least an annual assessment of cyber assets is required to determine if reliability standards have been met. These can be accomplished by entity self-assessments.

4.2.3.5. FERC Summary

FERC developments are regulatory in nature. Regulations come after all voluntary methods have been attempted, but have failed. When an event such as a major power outage makes it clear that voluntary measures to secure the bulk-power grid system are unsuccessful, then FERC creates legislation to solve the

problem. FERC has also tried to improve information sharing by creating more specific rules protecting the access and availability of critical infrastructure information submitted to the government. However, resistance to sharing sensitive, potentially damaging information with the government still exists.

CHAPTER 5. DISCUSSION

5.1. Themes

There are three main reoccurring themes that appear in each group of developments. These themes involve reaction to major power outages, the role of money in business decisions, and the constant emphasis on public-private partnership information sharing.

5.1.1. Power Outages

Major power outages bring attention to the vulnerabilities of the bulk-power grid system and the fact that reliability standards are not being implemented. The lack of adoption of voluntary reliability standards points to the need for regulation.

Cyber critical infrastructure protection efforts appear to intensify after a major power outage. Power outages are reported to NERC and the DOE. These reports are called electricity disturbance reports. An examination of the data in these reports show trends involving power outages (see Appendix B). When the number of outages per year increases the likelihood for a major power outage also appears to increase. Both NERC and the DOE show larger numbers of power outages occurring per year during 2003 through 2006 (numbering from 60-90 per year). One to three major power outages per year also occurred during this timeframe. Looking at the developments that occurred from 2003-2007, there was a plethora of activity, including regulations, standards, and plans (See table 1 in Chapter 4).

The economic impact adds an additional motivation to protection efforts. The cost of a major blackout can be in the billions of dollars. For example, the

worst blackout in recent history in the United States occurred in the summer of 2003. The cost of the Northeast Blackout ranged from $7-10 billion dollars (Natural Resources Canada & U.S. Department of Energy, 2006).

This major power outage resulted in increased efforts to achieve a sustained level of electricity generation and transmission reliability in the bulk-power grid system. The critical infrastructure developments in response to this major power outage are the following:

- *Energy Policy Act* of 2005
- NERC become ERO in 2006
- NERC submits cyber critical infrastructure standard to FERC to be approved
- FERC approved the *Mandatory Reliability Standards on Critical Infrastructure Protection* in 2008

Major power outages show that security guidelines and reliability standards are not being implemented on a voluntary basis in the electricity sector. This begs the question why? The answer appears to lie with economic considerations.

5.1.2. Economic Considerations

Since the majority of the cyber critical infrastructure is owned by the private sector it is important for the public sector to understand the role of economics in business decisions. The concept of return on investment and cost benefit analysis are used when considering new business expenditures. If the financial analysis shows poor returns to no returns then why should a business invest in additional security measures? The answer is that businesses will avoid investing in additional security.

If an entity within the electricity sector experiences a cyber attack that is significantly financially damaging then they will take measures to prevent this from happening in the future (invest in counter measures such as cyber security).

However, if the risk is low for a successful, damaging cyber attack, and it is cheaper to clean up after an attack than install preventive measures, the organization will take the route that makes better business sense. These beliefs are seen in the *E-Crimes Survey*. In the survey spending decreased on information technology security measures (CSO et al., 2007).

The cost of securing control systems and SCADA system from cyber attacks is difficult to determine. Control systems according to DOE cost 3-4 billion dollars for the electric grid. Remote field devices cost 1.5-2.5 billion dollars to replace (GAO, 2007a, p. 7). Retrofitting existing SCADA system is also probably an expensive expenditure (estimated 1/2 – 1 million dollars).

The GAO did a cost report on the *Mandatory Reliability Standards for Critical Infrastructure Protection*. Just the cost for information gathering requirements will amount to more than $100 million to meet full critical infrastructure compliance (GAO, 2008). This does not even take into account the cost of actual implementation expenses associated with compliance. If the investment is so high, some electricity entities might decide not to comply. To counteract this scenario the penalty fees are set to a maximum of 1 million dollars per day (GAO, 2007a).

Since 1,000 entities within the electricity sector need to comply with *Mandatory Reliability Standards for Critical Infrastructure Protection* and if information gathering costs is 10% of total compliance cost, then each entity is looking at a cost of 1 million dollars or more. 632 of these entities are classified as small businesses and a security expense of 1 million dollars or more might not be economically feasible.

The resistance to complying with voluntary standards created by NERC was probably due to the high price of compliance. There were several compliance reports by NERC on voluntary reliability standards. For the second quarter of 2007, 3,412 violations were reported (self-reported) (NERC, 2007a). Entities can self-certify that they have met compliance. These compliance reports occurred before the *Mandatory Reliability Standards for Critical Infrastructure*

Protection was put into effect. There have been no new compliance reports as of March 2008.

The resistance to sharing potentially damaging information with the DHS can also be tied to economics. GAO confirms that the financial risks of sharing critical infrastructure information can be determined, but the benefits are not easy to determine for the private sector (GAO, 2004a). These risks can encompass customers losing confidence, lawsuits, loss of business, and decreases in stock prices.

The GAO report on *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information*, clearly shows that DHS has received a total of 290 submissions (up till Jan 2006) from the private sector (GAO, 2006). GAO also reported that DHS has not used the information submitted by the private sector to issue any warnings or advisories, which makes the private sector wonder what the information is used for (GAO, 2006). Additionally, there has been no court case to uphold protection of submitted information from the Freedom of Information Act (GAO, 2006). Without the legal precedent set, the private sector still sees sharing information with the DHS as a risk without much benefit and since information sharing is voluntary, the private sector tends to abstain. This hints at underlying problems with the public-private partnership.

5.1.3. Public-Private Partnership Efforts

Building effective partnerships requires trust, mutual goals, and recognized benefits of working together. The *Critical Foundations* report along with all the plans and strategies in the DHS group put emphasis on developing effective public-private partnerships. Partnerships efforts are seen between NERC and FERC in the development of standards for cyber critical infrastructure protection. However, the partnership efforts between NERC and DHS seem to be tenuous at best.

The partnership efforts between FERC and NERC are successful because they both hold equal responsibilities in creating and enforcing reliability standards. NERC creates the standard and FERC makes sure it is a well developed and reasonable before giving its official seal of approval. However, the relationship between DHS and the private entities that NERC represents is not that successful since the responsibilities and benefits are not clearly recognized.

DHS needs to make it clear why it needs cyber critical infrastructure information from the private sector. DHS needs to convey how this information is used, how this information is protected (who is authorized to access it), and show the benefits to the private sector of sharing information. GAO reports that DHS has not said if it needs specific vulnerability information or interdependencies and this drives the question if DHS knows what it needs (GAO, 2006). More specific questions and requests communicates that DHS knows what it is doing. What information should the private sector submit, what is meaningful and what is not. GAO reported in 2006 that this is not clear (GAO, 2006). Additionally GAO reports that benefits to sharing information have not been demonstrated. For example providing the analytical processes (combining vulnerability, threat, and incident information that can be applied) would benefit the private sector, but this is not one of the services that the government can provide to the private sector at this time (GAO, 2004b).

The concept of DHS as a focal point for disseminating information is a good idea. This ensures that all participants get the information in a timely manner. Not having a focal point for information dissemination will result in duplicate and inefficient efforts. It is important to get key information into the hands of people who can mitigate the damage, and those people are in the private sector, not the public sector. The public-private partnership efforts would be improved if DHS could deliver relevant, processed, timely information to the private sector.

In 2007 GAO reported on information sharing by the DHS to the privates sector on cyber critical infrastructure. From 2003 to June, 2006, DHS has only

issued nine notices on control system vulnerabilities to the private sector (GAO, 2007a). This small number of notices does not encourage the private sector to reciprocate information sharing with the DHS.

DHS information sharing capabilities are further restricted by organization issues within DHS. Not only is employee turnover a problem, but also the requirement of informing congressional, agency and executive officials before communicating with the private sector. This results in delaying timely, relevant information sharing with the private sector. There is an additional difficulty of determining the right classification for the information and determining who can access it (GAO, 2007a).

DHS has lost many of its key positions during 2004 and 2005. The NCSD Director, the Director of US-CERT, the Under Secretary for Information Analysis and Infrastructure Protection Directorate, to name a few (GAO, 2005). The turnover in DHS leadership positions has produced an unstable environment, which results in the private sector wondering if the DHS is capable. The lack of maintenance in the PCII Program's Web page points to probable organizational problems within the DHS (See Figure 3 for expired certificate). This unstable environment is not conducive to building or maintaining trusted relationships between the private sector and the DHS.

GAO also reported in 2007 that there still was no standard governmental implemented process for sharing information with the private sector. Challenges still persist in developing productive public-private partnerships, especially in regards to information sharing (GAO, 2007b).

Many of the plans and strategies also mentioned that a coordinated effort between the public sector and the private sector was put into creating the actual document. However, GAO reported that "DHS has often informed the infrastructure sectors about government initiatives or sought input after most key decisions have been made."(GAO, 2005 p. 57, ¶ 3) The only plan that really showed a coordinated effort between NERC, DHS, and DOE was the Roadmap Report in 2007.

CHAPTER 6. CONCLUSION

Deciphering the cyber critical infrastructure protection efforts over the last eleven years is similar to putting together a puzzle. There are many pieces that individually do not appear that meaningful but when they are combined together a complete picture emerges. In this research all the cyber critical infrastructure developments are pieces in the puzzle. When all the pieces are sorted and put into their correct location, the puzzle forms a picture of protective efforts to secure the bulk-power grid system from cyber attacks over the eleven year timeframe. This picture provides perspective on what efforts have been successful and what efforts have not. The picture also shows the reoccurring themes that influence cyber critical infrastructure protection efforts over the time period.

To make sense of all the developments over the 11 years, these developments were sorted into three groups: DHS, NERC, and FERC. Each group was analyzed to determine the evolution of developments and for the evidence of any reoccurring themes. The evolution of efforts is important because it shows if developments build on top of each other or if they are being reinvented. The ability to improve is based on learning from past events by building on successes and learning from failures. The developments by NERC showed a real evolution of efforts, building on top of the previous developments, by refinement. DHS also showed plans building on plans, however, the plans rehash the contents of previous plans and added little improvement, the only exception was the Roadmap Report.

Analyzing these past developments over time also shows the presence of persisting underlying themes. Reoccurring themes are indicative of unresolved

issues. It is important to identify these issues so efforts in the future can focus on solving them. The three major themes identified in this research are the stimulus role of major power outages, the resistance to investing in security, and the lack of effective partnership efforts.

The DHS' role is to be the focal point/coordinator of critical infrastructure protection efforts. To accomplish this, effective partnerships between the public and private sectors is required. DHS has only been around since 2003. Being the focal point of critical infrastructure protection efforts is a mammoth project and takes time to accomplish. As a new organization, DHS has been plagued by organizational and implementation issues. Employee turnover, not producing plans on schedule, and not establishing effective processes for information sharing have been problems. These shortcomings do not inspire trust in the private sector. The goals set out in the plans all involve public-private partnership efforts, however the private sector has not experienced any benefit yet to this arrangement.

The private sector is represented by NERC. NERC's goal is to help establish power grid reliability. It does this by providing guidelines to secure systems, instructional manuals on how to create standards, and implementation guidelines with dates for compliance and progress checks. To achieve cyber security reliability in the bulk-power grid system the electricity sector needs to invest in implementing security measures. To reconfigure existing technology such as SCADA systems or set up new secure computer system is a significant expense. Entities within the electricity sector are resistant to investing in security when the return on investment is questionable. This resulted in regulation to force compliance to cyber security standards.

FERC's role is to promote a robust infrastructure that provides a reliable level generation and distribution of electricity. It does this by regulating the electricity sector. When a major power outage happens FERC responds by taking the needed measures to prevent similar events from occurring in the future.

FERC was given more authority after the Northeast Blackout of 2003. The blackout showed that private sector was not voluntarily adopting NERC's reliability standards. FERC certified NERC as the ERO to develop and enforce standards. In order to protect the cyber critical infrastructure from cyber attack, FERC passed the *Mandatory Reliability Standards for Critical Infrastructure Protection* in 2008.

Some progress in securing the bulk-power grid system from cyber attacks has occurred over the last eleven years. Plans have been made and standards have been created. The compliance to standards will not be known until 2011 when the audits have all been completed.

Electricity sector buy-in and effective public-private partnerships are needed to achieve a sustained level of cyber critical infrastructure protection. This goal will always be a moving target. Nothing can be completely 100% secure from cyber attack, due to the changing nature of technology and evolving modes of attack. Only through constant evaluation, testing (e.g., cyber attack scenario exercises), and updating security can the threat of cyber attacks be controlled, but the threat can never be complete eliminated.

Cyber critical infrastructure protection efforts of the bulk-power grid system are just at the beginning of a long journey. Work needs to done on implementing standards and building effective information sharing partnerships. Time will tell if efforts are effective at protecting the bulk-power grid from cyber attacks.

REFERENCES

Byres, E. & Lowe, J. (2004). *The myths and facts behind cyber security risks for industrial control systems*. Retrieved January 22, 2008, from http://tswg.gov/subgroups/ps/infrastructure-protection/documents/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf

CSO Magazine, U.S. Secret Service, CERT Program, and Microsoft Corporation. (2007). *2007 e-crime watch survey*. Retrieved February 11, 2008, from http://www.cert.org/archive/pdf/ecrimesummary07.pdf.

Cyber Security Industry Alliance. (2008). *SCADA: get the facts*. Retrieved January 23, 2008, from http://www.csialliance.org/issues/scada/.

Department of Homeland Security. (2006a). *National infrastructure protection plan*. Retrieved February 1, 2008, from http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Department of Homeland Security. (2006b). *Protected critical infrastructure information (PCII) program*. Retrieved January 21, 2008, from http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm.

Department of Homeland Security. (2007). *National infrastructure protection plan*. Retrieved July 27, 2007, from http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Department of Homeland Security & Department of Energy. (2006). *Roadmap to secure control systems in the energy sector*. Prepared by Energetics Incorporated, Columbia, Maryland. Retrieved March 3, 2008, from http://www.oe.energy.gov/DocumentsandMedia/roadmap.pdf.

Department of Homeland Security & Department of Energy. (2007). *Energy: critical infrastructure and key resources sector-specific plan as input to the national infrastructure protection plan (redacted)*. Retrieved March 1, 2008, from ftp://ftp.nerc.com/pub/sys/all_updl/cip/Energy_Redacted_All.pdf.

Donahue, Tom. (2008). *CIA confirms cyber attack caused multi-city power outage*. SANS Process Control and SCADA Security Summit, in New Orleans, Louisiana. Retrieved on March 11, 2008, from SANS.org Web site: http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5.

Electricity Sector Information Sharing and Analysis Center. (2007). *ESISAC*. Retrieved March 12, 2008, from http://www.esisac.com/.

Energy Information Administration. (2008). *United States electricity facts: a summary*. Retrieved March 16, 2008, from http://www.eia.doe.gov/neic/a-z/elsum.htm.

Energy Policy Act. (2005). *Public Law 109-58*, 109th Congress. 42 USC 15801. Retrieved January 4, 2008, from http://www.epa.gov/OUST/fedlaws/publ_109-058.pdf.

Freedom of Information Act. (2002). *5 U.S.C. § 552*. Retrieved on March 5, 2008, from USDOJ.gov Web site: http://www.usdoj.gov/oip/foiastat.htm.

Government Accountability Office. (2004a). *Critical infrastructure protection: establishing effective information sharing with infrastructure sectors*. Retrieved February 20, 2008, from http://www.gao.gov/new.items/d04699t.pdf.

Government Accountability Office. (2004b). *Critical infrastructure protection: improving information sharing with infrastructure sectors*. Retrieved February 20, 2008, from http://www.gao.gov/new.items/d04780.pdf.

Government Accountability Office. (2005). *Critical infrastructure protection: department of homeland security faces challenges in fulfilling cybersecurity responsibilities*. Retrieved February 20, 2008, from http://www.gao.gov/new.items/d05434.pdf.

Government Accountability Office. (2006). *Information sharing: DHS should take steps to encourage more widespread use of its program to protect and share critical infrastructure information*. Retrieved February 20, 2008, from http://www.gao.gov/new.items/d06383.pdf.

Government Accountability Office. (2007a). *Critical infrastructure protection: Multiple efforts to secure control systems are under way, but challenges remain*. Retrieved February 26, 2008, from http://www.gao.gov/new.items/d071036.pdf.

Government Accountability Office. (2007b). *Department of homeland security: progress report on implementation of mission and management functions*. Retrieved February 26, 2008, from http://www.gao.gov/new.items/d071240t.pdf.

Government Accountability Office. (2007c). *Critical infrastructure protection: multiple efforts to secure control systems are under way, but challenges remain*. Retrieved March 11, 2008, from http://www.gao.gov/new.items/d08119t.pdf

Government Accountability Office. (2008). *Report under 5 U.S.C. § 801(a)(2)(a) on a major rule issued by the department of energy, federal energy regulatory commission entitled "mandatory reliability standards for critical infrastructure protection"* (Docket No. RM06-22-000). Retrieved March 7, 2008, from http://www.gao.gov/decisions/majrule/d08493r.pdf.

Hilt, D. W. (2006). *Impacts and actions resulting from the August 14, 2003 blackout*. Retrieved May 22, 2007, from ftp://www.nerc.com/pub/sys/all_updl/docs/blackout/ISPE%20Presentation%20-%20Impacts%20and%20Actions%20Resulting%20from%20the%20August%2014%20Blackout.pdf.

Homeland Security Act. (2002). *Public Law 107-296*, 107th Congress, 116 STAT. 2135. Retrieved February 15, 2008, from http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

H.R. 5005-11. (2002) *Title II—Information Analysis and Infrastructure Protection*. Retrieved March 2, 2008, from http://www.dhs.gov/xlibrary/assets/CII_Act.pdf.

Leffler, L. (2002). *Discussing activities undertaken by the electricity sector to address physical and cyber security with emphasis on the electricity sector – information sharing and analysis center (ES-ISAC): Testimony before the Committee on Governmental Reform, Subcommittee on Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations*, United States House of Representatives. Retrieved March 13, 2008, from http://www.esisac.com/publicdocs/HouseCommitteeonGovtReform072402.pdf.

National Commission on Terrorist Attacks. (2004). *The 9/11 commission report*. Retrieved February 2, 2008, from http://www.gpoaccess.gov/911/pdf/fullreport.pdf.

National Oceanic and Atmospheric Administration. (2003). *NOAA posts images online of northeast blackout.* Retrieved April 13, 2008 from http://www.noaanews.noaa.gov/stories/s2015.htm

Natural Resources Canada & U.S. Department of Energy. (2006). *Final report on the implementation of the task force recommendations*. Retrieved May 22, 2007, from http://www.ferc.gov/industries/electric/indus-act/blackout/09-06-final-report.pdf#xml=http://search.atomz.com/search/pdfhelper.tk?sp_o=4,100000,0.

North American Electric Reliability Corporation. (2007c). *Compliance monitoring and enforcement program 2008 implementation plan*. Retrieved March 17, 2008, from ftp://www.nerc.com/pub/sys/all_updl/compliance/NERC_2008_Annual_Implementation_Plan_Version_1-7.pdf.

North American Electric Reliability Corporation. (2007e). *Reliability standards development plan: 2008–2010*. Retrieved March 7, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/sar/FERC_Filing_Volumes_I_II_III_Reliability_Standards_Development_Plan_2008_2010.pdf.

North American Electric Reliability Corporation. (2008a). *Reliability standards*. Retrieved March 7, 2008, from http://www.nerc.com/~filez/standards/Reliability_Standards_Regulatory_Approved.html.

North American Electric Reliability Corporation. (2008b). *Events analysis*. Retrieved March 14, 2008, from http://www.nerc.com/~filez/disturbancereports.html.

North American Electric Reliability Corporation. (2008c). *U.S. department of energy incident and disturbance reporting requirements*. Retrieved March 3, 2008, from http://www.nerc.com/~dawg/append-a.html.

North American Electric Reliability Corporation. (2008d). *About NERC*. Retrieved March 13, 2008, from http://www.nerc.com/about/.

North American Electric Reliability Corporation. (2008f). *About NERC FAQ*. Retrieved January 6, 2008, from http://www.nerc.com/about/faq.html#How_is_NERC_funded.

North American Electric Reliability Council. (2002a). *Proposed rule regarding critical energy infrastructure information*. (Docket No. RM02-4-000, PL02-

1-000). Retrieved March 13, 2008, from ftp://www.nerc.com/pub/sys/all_updl/cip/NERC_RM02_4_CEII.pdf.

North American Electric Reliability Council. (2002b). *Security guidelines for the electricity sector*. (Electricity Market Design and Structure Docket No. RM01-12-000). United States of America Federal Energy Regulatory Commission. Retrieved January 1, 2008, from: http://www.esisac.com/publicdocs/Guides/SecurityGuidelinesElectricitySector-Version1.pdf.

North American Electric Reliability Council. (2003a). *NERC reliability standards process manual*. Retrieved March 18, 2008, from ftp://ftp.nerc.com/pub/sys/all_updl/oc/stp/RSPM_V2.1_Final.pdf.

North American Electric Reliability Council. (2003c). *Urgent action standard 1200 - cyber security*. Retrieved March 3, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Urgent_Action_Standard_1200_Cyber_Security.pdf.

North American Electric Reliability Council. (2005). *Critical infrastructure protection — cyber security standards development highlights*. Retrieved March 3, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Development_Highlights_Final.pdf.

North American Electric Reliability Council. (2006a). *(Revised) implementation plan for cyber security standards cip-002-1 through cip-009-1*. Retrieved March 5, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Revised_Implementation_Plan_CIP-002-009.pdf.

North American Electric Reliability Council. (2006b). *Standard CIP–002–1 — cyber security — critical cyber asset identification*. Retrieved March 5, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-002-1.pdf.

North American Electric Reliability Council. (2006c). *Standard CIP–003–1 — cyber security — security management controls*. Retrieved March 5, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-003-1.pdf.

North American Electric Reliability Council. (2006d). *Standard CIP–004–1 — cyber security — personnel and training*. Retrieved March 5, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-004-1.pdf.

North American Electric Reliability Council. (2006e). *Standard CIP–005–1 — cyber security — electronic security perimeter(s)*. Retrieved March 5, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-005-1.pdf.

North American Electric Reliability Council. (2006f). *Standard CIP–006–1 — cyber security — physical security of critical cyber assets*. Retrieved March 5, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-006-1.pdf.

North American Electric Reliability Council. (2006g). *Standard CIP–007–1 — cyber security — systems security management*. Retrieved March 5, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-007-1.pdf.

North American Electric Reliability Council. (2006h). *Standard CIP–008–1 — cyber security — incident reporting and response planning*. Retrieved March 5, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-008-1.pdf.

North American Electric Reliability Council. (2006i). *Standard CIP–009–1 — cyber security — recovery plans for critical cyber assets*. Retrieved March 5, 2008, from ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-009-1.pdf.

North American Electric Reliability Council. (2006j). *Reliability standards development procedure*. Retrieved March 13, 2008, from ftp://ftp.nerc.com/pub/sys/all_updl/oc/stp/RSDP_V6_01Nov06.pdf.

Office of Homeland Security. (2002). *National strategy for homeland security*. Retrieved January 22, 2008, from http://www.oe.energy.gov/DocumentsandMedia/National_Strategy_for_Homeland_Security.pdf.

Poulsen, K. (2005). *U.S. info-sharing initiative called a flop*. Retrieved March 15, 2008, from http://www.securityfocus.com/news/10481.

President's Commission on Critical Infrastructure Protection. (1997). *Critical foundations: protecting America's infrastructures*. Retrieved March 10, 2008, from http://www.ihs.gov/misc/links_gateway/download.cfm?doc_id=327&app_dir_id=4&doc_file=PCCIP_Report.pdf.

Sandia Corporation. (n.d.). *Frequently asked questions*. Retrieved Jan 4, 2008, from http://www.sandia.gov/scada/faq.htm.

The White House. (1998). *Presidential decision directive/NSC-63*. Retrieved March 2, 2008, from http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf.

The White House. (2003a). *National strategy to secure cyberspace*. Retrieved January 24, 2008, from http://www.oe.energy.gov/DocumentsandMedia/National_Strategy_to_Secure_Cyberspace.pdf.

The White House. (2003b). *Homeland security presidential directive/HSPD-7*. Retrieved February 4, 2008, from http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

U.S.-Canada Power System Outage Task Force. (2004). *Final report on the August 14th blackout in the United States and Canada: causes and recommendations (Final Blackout Report)*. Retrieved January 2, 2008, from http://www.ferc.gov/cust-protect/moi/blackout.asp.

U.S. Computer Emergency Readiness Team. (2008). *Welcome to US-CERT*. Retrieved March 12, 2008, from http://www.us-cert.gov/.

United States Department of Energy Federal Energy Regulatory Commission. (2003). *Critical Energy Infrastructure Information, Final Rule, 18 CFR Parts 375 and 388*, Federal Register, Rules and Regulations, Vol. 68, No. 41, pp. 9857-9873. Retrieved December 1, 2007, from http://www.fas.org/sgp/news/2003/03/fr030303.pdf.

United States of America Federal Energy Regulatory Commission. (2004). Policy statement on matters related to bulk power system reliability. (Docket No. PL04-5-000; 107 FERC ¶ 61,052). Retrieved March 14, 2008, from ftp://ftp.nerc.com/pub/sys/all_updl/docs/ferc/Rx-Policy-statement.pdf.

United States of America Federal Energy Regulatory Commission. (2007). *Mandatory Reliability Standards for the Bulk-Power System. Final Rule*. (Docket No. RM06-16-000; Order No. 693. 18 CFR Part 40). Retrieved March 15, 2008, from ftp://ftp.nerc.com/pub/sys/all_updl/docs/ferc/order_693.pdf.

United States of America Federal Energy Regulatory Commission. (2007b). *Annual report 2006.* Retrieved March 23, 2008 from: http://www.ferc.gov/about/strat-docs/fy06-an-rpt.pdf

United States of America Federal Energy Regulatory Commission. (2008a). *Mandatory reliability standards for critical infrastructure protection. Final Rule*. (Docket No. RM06-22-000; Order No. 706. 18 CFR Part 40. 122

FERC ¶ 61,040). Retrieved March 15, 2008, from ftp://ftp.nerc.com/pub/sys/all_updl/docs/ferc/Order_706.pdf.

United States of America Federal Energy Regulatory Commission. (2008b). *FERC approves new reliability standards for cyber security*. Retrieved March 1, 2008, from http://www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.asp.

Appendix A. Mandatory CIP Standards

The cyber critical infrastructure reliability standards became effective June 1, 2006 and mandatory full compliance is due by 2010 (NERC, 2006a). Compliance is shown by documentary evidence that the requirements in each standard have been met. The following is a quick overview of the Cyber Security Standards CIP-002-1 through CIP-009-1 (Tables A.1 to.A.8).

Table A.1 CIP-002

Name	Cyber Security — Critical Cyber Asset Identification (NERC, 2006b)
Description	Risk-based methodology to identify assets
Requirement 1	Critical asset identification method developed
Requirement 2	List of critical assets
Requirement 3	List of critical cyber assets that correspond to list of critical assets
Requirement 4	Annual approval by senior management of the lists

Table A.2 CIP-003

Name	Cyber Security — Security Management Controls (NERC, 2006c)
Description	Have minimum security management controls in place to protect critical cyber assets
Requirement 1	Cyber security policy
Requirement 2	Leaderships for managing implementation of CIP-002 through CIP-009
Requirement 3	Exceptions to security policy must be documented
Requirement 4	Information protection program (identify, classify, and protect information)
Requirement 5	Access control program to protect information
Requirement 6	Establish a process for adding, modifying, replacing, and removing critical cyber assets

Table A.3 CIP-004

Name	Cyber Security — Personnel and Training
Description	Personnel having access to cyber critical assets have the appropriate clearance level (NERC, 2006d)
Requirement 1	Establish and maintain annual cyber security training
Requirement 2	Establish and maintain security awareness program
Requirement 3	Information protection program (identify, classify, and protect information)
Requirement 4	Personnel risk assessment (background investigation)
Requirement 5	List of personnel with access to cyber critical assets

Table A.4 CIP-005

Name	Cyber Security — Electronic Security Perimeter(s) (NERC, 2006e)
Description	Identification and protection of critical cyber assets by defining the security perimeter and access points
Requirement 1	Every critical cyber asset resides within an electronic security perimeter
Requirement 2	Electronic access controls
Requirement 3	Monitor and log electronic access
Requirement 4	Cyber vulnerability assessments on electronic access points at least annually
Requirement 5	Document efforts and keep logs at least 90 days

Table A.5 CIP-006

Name	Cyber Security — Physical Security (NERC, 2006f)
Description	The physical security program for critical cyber assets
Requirement 1	Physical security plan
Requirement 2	Physical access controls procedural controls
Requirement 3	Monitor physical access
Requirement 4	Logging physical access
Requirement 5	Access log retained for at least 90 days
Requirement 6	Maintenance and testing to ensure physical security systems work correctly

Table A.6 CIP-007

Name	Cyber Security — Systems Security Management (NERC, 2006g)
Description	Define methods, processes, and procedures for securing systems that are classified as critical cyber assets
Requirement 1	new cyber assets and changes to existing cyber assets shall not adversely affect existing cyber security controls
Requirement 2	only ports and services required for normal operations are enabled
Requirement 3	security patch management
Requirement 4	malicious software prevention (use anti-virus and other malware prevention tools)
Requirement 5	account management to enforce access authentication, accountability for all user activity
Requirement 6	security status monitoring
Requirement 7	formal methods for disposal or redeployment of cyber assets
Requirement 8	cyber vulnerability assessment (at least annually)
Requirement 9	documentation review and maintenance

Table A.7 CIP-008

Name	Cyber Security — Incident Reporting and Response Planning (NERC, 2006h)
Description	Identification, classification, response, and reporting of incidents relating to critical cyber assets
Requirement 1	create and annually review recovery plans
Requirement 2	the recovery plans shall be exercised at least on an annual basis

Table A.8 CIP-009

Name	Cyber Security — Recovery Plans for Critical Cyber Assets (NERC, 2006i)
Description	Recovery plans put in place for critical cyber assets that conform to business continuity and disaster recovery practices
Requirement 1	create and annually review recovery plans
Requirement 2	the recovery plans shall be exercised at least on an annual basis

Appendix B. Power Grid Disturbances

Tracking power outages or disturbances to the power grid system is important because analyzing the data over a substantial period of time will provide information about trends. Both DOE and NERC compile information on power grid disturbances. However, they both only report a selected subset of all disturbances reported. To compare the data from the two groups, a major power outage for the purposes of this research is one that affects over one-million customers.

The DOE has mandatory reporting requirements for electric disturbances. A report must be filed within one-hour of an incident when the following occurs (NERC, 2008c):

- Loss ≥300 MW for ≥15 minutes
- Load shedding of ≥100 MW
- System-wide voltage reduction of ≥3%
- Public appeal to reduce use of electricity
- Actual or suspected physical attack
- Actual or suspected cyber and/or communication attack
- Fuel supply emergency
- Loss of service to ≥50,000 customers for ≥1 hour
- Complete operational failure or shut-down of the transmission and/or distribution system

This reporting requirement was made mandatory under the Federal Energy Administration Act of 1974 and failure to comply results in monetary fines of up to $5,000 per day (NERC, 2008c). The DOE Energy Information Administration (EIA) compiles the disturbance reports and incorporates them into their EIA Electric Power Monthly documents (Energy Information Administration, 2008). A graph (Figure B.1) on the power outages reported to DOE shows outages peaking in 2004 and a slight decline from 2004 through 2007.

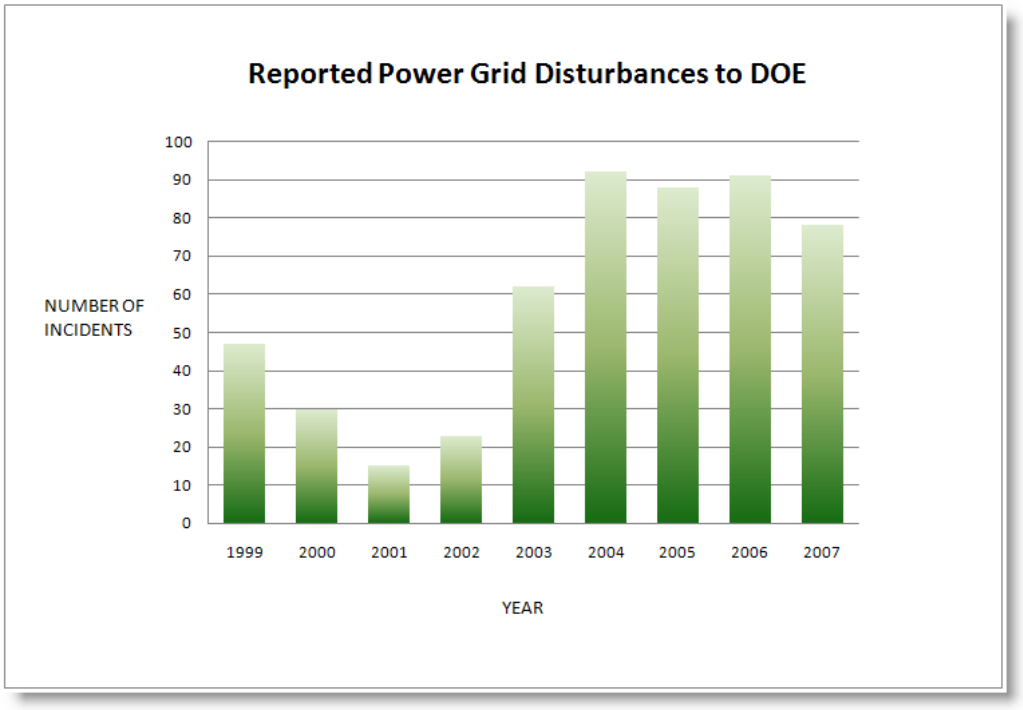

Figure B.1 Power Grid Disturbances per year reported by DOE

NERC maintains a database of disturbances reported to them on a voluntary basis. Their information is a little more descriptive on the suspected causes of the disturbance. In regards to cyber security, SCADA failures contributing to the power outages in five out of the eleven years of disturbance reports (NERC, 2008b). An increasing trend of number of power outages per year can be seen in Figure B.2.

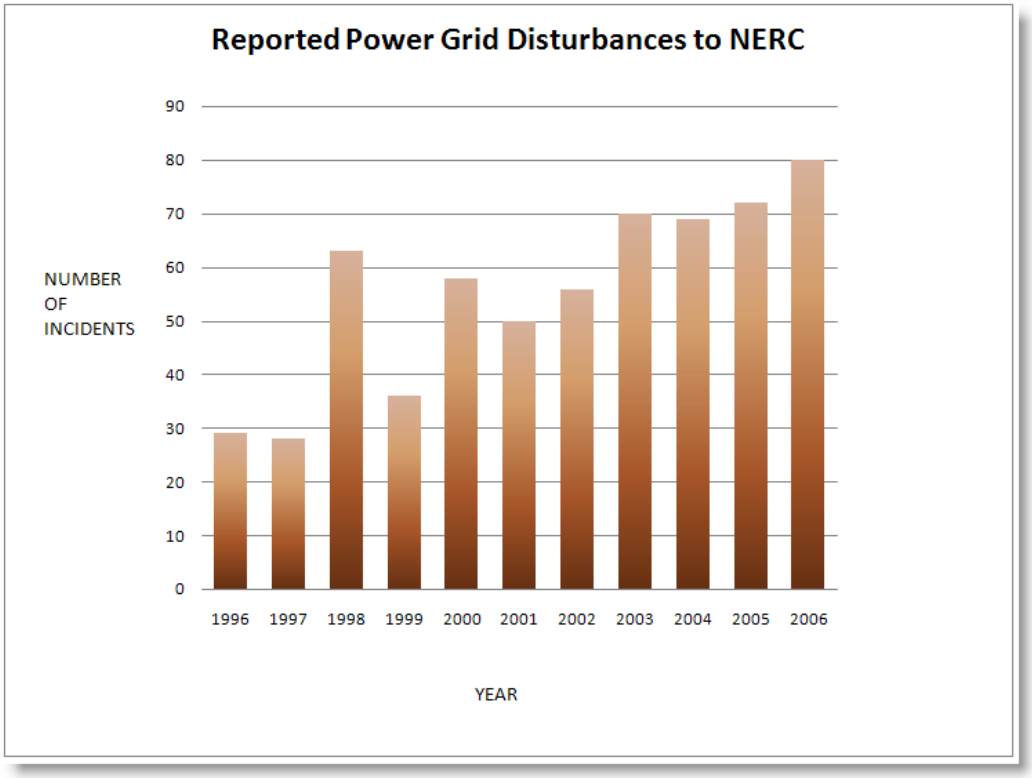

Figure B.2 Power Disturbance per year reported to NERC

Comparing major power outages (≥1 Million customers affected) between the data sets of DOE and NERC show a constant pattern of 1-3 major power outages per year from 2002-2006 (Figure B.3).

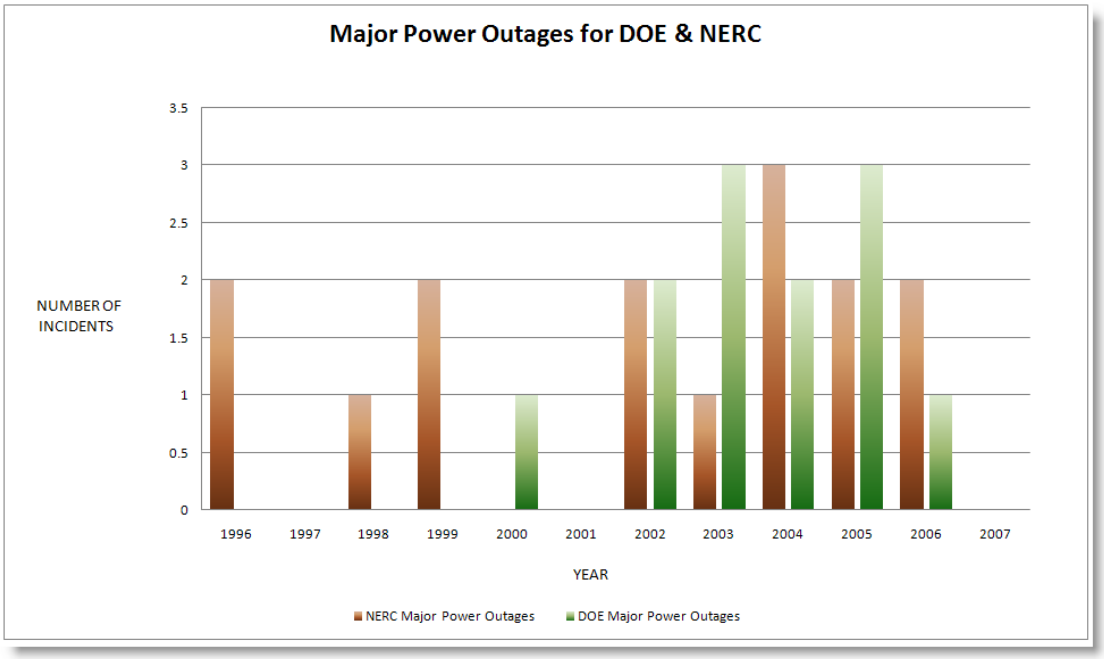

Figure B.3 Major Power Outages

REFERENCES

APPENDICES