1999

Critical Infrastructure Assurance: Electric Power Reliability

A Report for Mitretek Systems Inc.
By: Max Bremer, Daniel Feliz, and Troy Perry

Abstract

In this policy analysis exercise (PAE), we analyze the North American electric power infrastructure and offer recommendations for reducing vulnerabilities. We examine the electric power industry, the threats to it, its vulnerabilities, and its relationships with other organizations. Our major sources of information consist of interviews, attendance at an infrastructure protection conference, and extensive academic research. Our recommendations focus on reducing three specific vulnerabilities: physical terrorism, cyber attacks and confluence of events. Finally, we assess the benefits of our recommendations and the obstacles to implementation.

Executive Summary

The Problem

The United States has one of the most reliable electric power systems in the world. However, recent changes in the electric power industry environment have given rise to increased vulnerabilities to a number of threats, including terrorist attack that could cause widespread electric power failure. These changes include industry deregulation, increased availability of information (from FOIA and the internet), increased dependence on information networks, and an increase in external, malevolent threats. Industry deregulation creates problems in the short term because it remains unclear which industry participants have responsibility for specific parts of the infrastructure. In order to reduce vulnerabilities and to maintain a reliable system, it is imperative that key players, including private industry, government, and non-government entities, take immediate action.

The Electric Power Industry: A Vital National Interest

The electric power industry represents a vital national interest. Other national critical infrastructures, as well as individuals, count on its continuing availability and reliability. Any massive failure of the electric power infrastructure would cause severe physical, economic and political hardships.

Scope of Project

Due to time, space, and availability of information constraints, we limit the scope of this project to three classes of vulnerabilities:

- Physical Terrorism
- Cyber Attacks
- Confluence of Events

Key Recommendations

1) Establish a regulatory and oversight organization, the North American Power Assurance Council (NAPAC), to replace NERC.
2) Clearly delineate responsibility for security
3) Implement Red Team security testing
4) Create the first Information Sharing and Analysis Center (ISAC), as mandated by President Clinton in PDD 63
5) Create and administer a modeling and simulation center
6) Conduct periodic, announced inspections
7) Legislate anti-trust exemptions for assurance corroboration

Table of Contents

Preface

On 10 August 1996 the Western Interconnection[1] had its second major power outage in as many months. Power trading and consumption were at near record levels in the Pacific Northwest when a sagging line in Oregon set in motion a cascading series of line failures. These failures led to generation imbalance, and then to the Western Interconnection being split into a set of four 'islands' of power. Unfortunately, the system that had been designed to optimize these islands was out of service, and the grid fractured into four uneven (power-wise) segments. This, in turn, led to millions of customers in 14 states and two Canadian provinces being without power for hours. Business shutdowns, transportation delays, and communication disruptions led to millions of dollars in losses. Furthermore, consumer confidence in the reliability of the electric power infrastructure was compromised.

The Northwest outage demonstrated vulnerabilities endemic throughout the electric power industry. First, with a near capacity load, one physical problem in the system led to additional physical problems. Then, a communications deficiency resulted in increased failures, which were then exacerbated by a malfunctioning safety program. Additionally, it showed how the confluence of several small incidents (events), not notable on their own, can combine to form a much more significant problem.

[1] An Interconnection is any one of the four electric system networks in North America: Eastern, Western, ERCOT and Alaska. Report on the Task Force on Electric System Reliability, Secretary of Energy Advisory Board, September 29, 1998, p. 47.

The Problem

The United States has one of the most reliable electric power systems in the world. However, recent changes in the electric power industry environment have caused an increase in overall vulnerability. These changes include industry deregulation, increased availability of information (from FOIA and the internet), increased dependence on information networks, and an increase in external, malevolent threats. Industry deregulation creates problems in the short term because it remains unclear which industry participants have responsibility for specific parts of the infrastructure. In order to reduce vulnerability and to maintain a reliable system, it is imperative that key players, mainly private industry, government and non-government entities, take immediate action. The purpose of this project is to analyze policy options that will support the electric power industry's efforts to improve assurance.

Overview

In this study we examine why the reliability of the electric power industry is a vital national interest, illustrate the major components of the industry, and discuss positive characteristics of the industry. We then discuss particular vulnerabilities and refine our focus to three areas of concern. Finally, we present our recommendations and show how they could reduce vulnerabilities, fix existing problems, or mitigate the consequences of these problems.

The Electric Power Industry: A Vital National Interest

What is infrastructure?

Infrastructure is the sum total of the acquired, in-place (not necessarily permanent) resources required for normal activity and economic growth. For the electric power industry, infrastructure includes the fuel supply system, power generation/ conversion equipment, buildings, cabling, transmission/distribution lines, and computer systems—all working in coordination—that make that industry unique in function. Our nation has a massive underpinning of infrastructure on which it is utterly dependent from day to day. Some infrastructure components are physical by nature, and some are tied more closely to the cyber world of information technology and data transfer. Critical infrastructures that this nation must protect include[2]:

- Electric power industry
- Telecommunication industry
- Banking and finance industry
- Transportation system
- Oil and gas delivery and storage system
- Water provision and distribution
- Emergency services and government

The extended compromise of any one of these systems would almost certainly cause severe economic, physical or political hardship for the country.

Why is the electric power industry vital?

The electric power industry is one of the most critical of our national

[2] President's Commission on Critical Infrastructure Protection Report, *Critical Foundations*, October, 1997.

infrastructures. According to Richard Clark, the National Security Council's National Coordinator for Security Infrastructure Protection and Counter-terrorism, "*The three most important national security infrastructures in the United States today are: electric utility, telecommunications, and transportation.*"[3] In defining critical infrastructure to which the limited resources available for protection should be allocated, it is important to start by looking at the reliance of the nation on the infrastructure, not the apparent proximity of the threat to the infrastructure itself. In other words, the immediacy of a threat has no bearing on the importance of the infrastructure. The electric power industry is vital to this country because the other national critical infrastructures, as well as individuals, count on its continuous, uninterrupted availability.

Because electric power is the keystone of all critical infrastructures, it must be made as secure as possible. As President Clinton stated on July 3, 1996, shortly after the first massive power outage of that year, "*A steady supply of power is a vital factor in both the local and national economies and is essential for the safety of all Americans.*" [4] Any massive failure of the electric power industry would have immediate consequences in the physical, economic and political realms. This ability to impact all three realms makes the electric power industry unique among infrastructures, as it has all three as immediate consequences.

Because it is a vital national interest, the electric power industry must be considered a high-priority target for terrorists. The diversity and relative size of the

---

[3] Richard Clark, Speech at Defense Week Conference on Defending National Critical Infrastructure, Washington D.C. December 7, 1998.

[4] Memorandum from President Clinton to Secretary of the Energy on July 3, 1996, as quoted in the Critical Infrastructure Assurance Office (CIAO) report, p. B-2.

vulnerable parts of the infrastructure make it exceptionally difficult to safeguard. Terrorists can attack small segments through cyber means, from within or outside the country. Even more terrifying is the new paradigm of terrorism focusing on inflicting severe economic or physical hardships that could lead to massive loss of life.[5] These terrorists, often state-supported, seek to develop weapons of mass destruction to this end. The destruction of the grid, even temporarily, combined with a chemical or biological attack, could be devastating. Thus, it is in our nation's interest to do everything possible to reduce vulnerability to terrorist attack.

What is assurance?

Assurance in the broadest sense involves taking all reasonable precautions to prevent or counter the known threats and mitigate known vulnerabilities. In the executive summary of the President's Commission on Critical Infrastructure Protection (PCCIP) report, the commission defines assurance as the industry "protecting [itself] against the tools of disruption."[6] Thus, an acceptable working definition of assurance involves confidence that reasonable protection against anticipated threats and known vulnerabilities has been implemented. The goal is increased reliability, since complete reliability (100%) can never be achieved due to limited resources and knowledge, and continuously changing threats and vulnerabilities.

[5] Office of the President. The Clinton Administration's Policy on Combating Terrorism: Presidential Decision Directive 62. May 22, 1998.
[6] President's Commission on Critical Infrastructure Protection Report, *Critical Foundations*, October, 1997, executive summary.

Characterization of the Infrastructure

Electric Power Industry

The electric power industry is actually a collection of three systems comprising the broad infrastructure. The three systems include power generation, transmission, and distribution. Energy providers who control the three systems fall into one of two categories:

- **Utilities**- Privately and publicly owned companies are engaged in the generation, transmission, and/or distribution of electric power. Examples of utilities include investor owned (e.g. Central Maine Power), federally owned (e.g. Tennessee Valley Authority), and publicly owned utilities (e.g. New York Power Authority).

- **Non-utilities**- Privately owned entities can generate power for their own use and sometimes for sale to other utilities. Non-utilities are important to energy industries like mining that cannot be serviced by utilities.

Power *vs.* Energy

Electric power is the rate at which electricity does work. The basic unit of measure is a watt.

Electric energy is the amount of electric power produced over time. The basic unit of measure is watt-hour.[7]

The **generation** component transforms stored energy into electric power. The generation sector is made up of coal, oil, gas, hydroelectric, nuclear, and a growing number of renewable (wind, solar, geothermal) generators throughout the US and Canada. There are about 10,400 generation units that are owned by investors, rural electric cooperatives, corporations, the federal government, local municipalities and independent power producers.[8] Generation is the most cost intensive part of the system both in terms of the cost of fuel and the assets needed to convert fuel. The federal

[7] Paul Tipler. Physics for Scientists and Engineers. Third Edition. Worth Publishing (1991), p. 3.
[8] *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures*, Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office, Washington, D.C., July 1998, p. B-3.

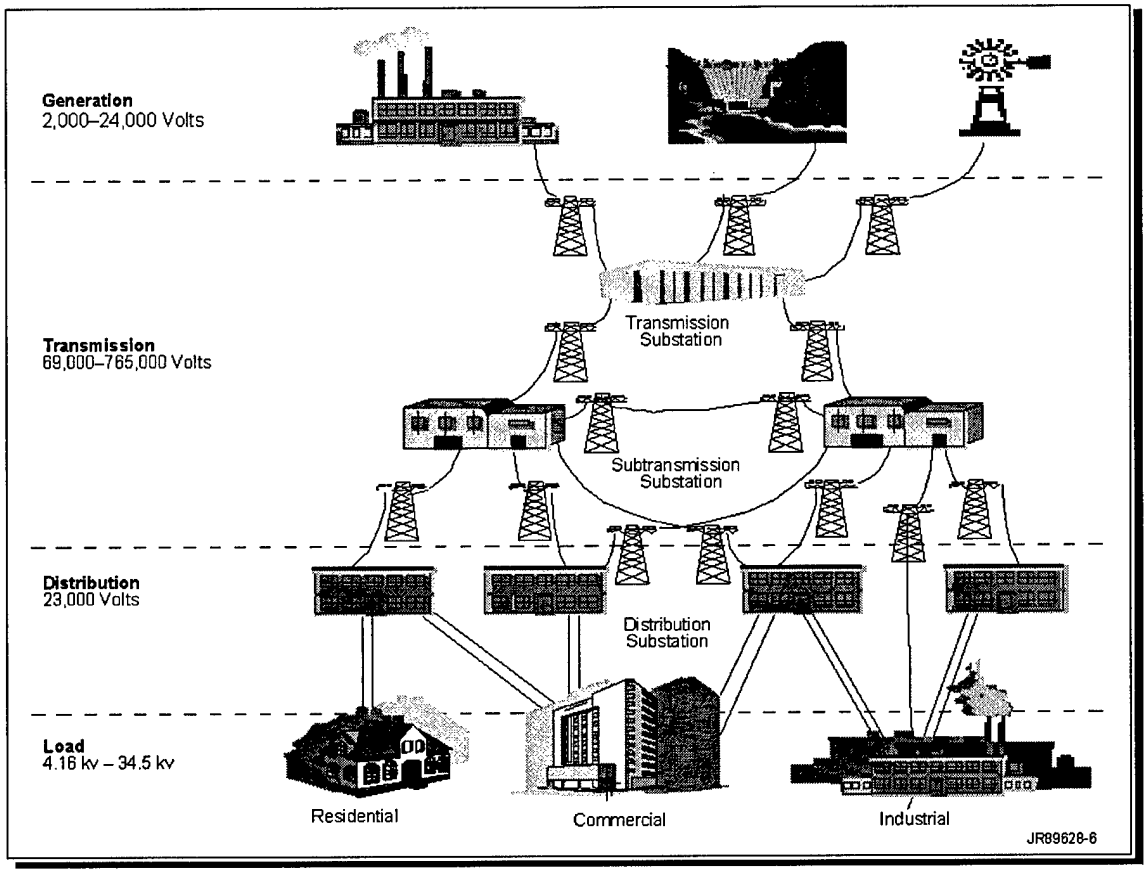
government (including TVA) has maintained a relatively large portion of market share in power generation over the past century. Currently the federal government produces 9% of all energy consumed in the country.[9] The majority of the remaining generators are now regulated, privately owned utilities.

The **transmission** system is what many would consider the real infrastructure. The transmission system is made up of a series of transformers that increase voltage from the generation source and feed it into the high voltage lines that carry this stepped-up voltage. These lines then feed substations or transformers that step down the voltage to a useable level. The large systems use alternating current (AC) that cycles sixty times every second because AC current can be easily stepped-up and down without major loss of current through automated means.[10] The automation of the transmission system makes it a prime target for terrorists since they do not have to contend with the security personnel.

The transmission system takes this generated power and delivers it to **distribution** systems. As Dr. Peter Fox-Penner points out, "the distribution system is usually considered to begin where the voltage is reduced to 37,000 volts."[11] The distribution system is highly automated but relatively diffuse and not as interdependent as the transmission system. For example, a single house blowing a fuse does not have any effect on the system.

---

[9] Department of Energy. The Changing Structure of Electric Power, 1999, p. 5.
[10] P.C. Sen. Principles of Electric Machines and Power Electronic. New York: Wiley and Sons. 1989, p. 545.
[11] Peter Fox-Penner, Electric Utilities Restructuring. Vienna, Va. Public Utility Reports, Inc: 1997. p. 23.



Source: NSTAC Information Assurance Task Forces, *Electric Power Risk Assessment 1998*, Fig. 2.

This chart illustrates the three main components of the electric power infrastructure: generation, transmission, and distribution.

Electric Power Reliability Organizations

Many governmental and non-governmental agencies are involved at various levels in the electric power industry. These entities include:

- **DOE** (Department of Energy)- A cabinet level federal agency overseeing energy policy. ***DOE develops long term strategy for managing national energy resources.*** DOE does have an electric system reliability task force that is currently examining reliability issues.

- **FERC** (Federal Energy Regulatory Commission) - A federal agency having jurisdiction over interstate transmission systems. Historically, FERC has regulated owners and operators of power transmission services to ensure nondiscriminatory service to all power suppliers and markets. Therefore, ***FERC focuses on universal access for consumers*** and has a limited role in regulating industry reliability standards.[12] FERC currently allows NERC to build industry consensus on reliability standards.

- **NERC** (North American Electric Reliability Council)- A voluntary private industry reliability organization created in 1968 to serve as an alternative to government regulation. ***NERC recommends standards and procedures to industry***, but has no enforcement authority. In other words, industry is not bound to follow its decisions. NERC's relative success hinges on industry's strong preference for addressing problems without government intervention.

- **CIAO** (Critical Infrastructure Assurance Office)- A new agency (created in 1998), ***CIAO is charged with developing a national plan for addressing physical and cyber threats*** to the nation's communications and electronic systems, transportation, energy, banking and financial, health and medical services, water supply, and key government services.

- **NIPC** (National Infrastructure Protection Center)- ***NIPC is the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures***. The FBI provides overarching control of NIPC.

- **RRC** (Regional Reliability Councils)- Voluntary reliability organizations (currently 10), ***RRCs monitor and assess regional criteria, guidelines, and procedures*** against NERC planning standards.

[12] William Young and Gregory Kinzelman, Regional Reliability: The Potential for Conflict Between Cooperation and Competition., p. 3.

A common objective (in various degrees) of these entities is codifying standards, procedures, and basic security measures to preserve the integrity of the infrastructure. Due to recent industry-wide deregulation, self-regulation from NERC and RRCs consensus-building forums have been the primary means of establishing industry standards and requirements. FERC and DOE regulation has been limited due to the wide success of RRCs in building consensus on important reliability issues like frequency, voltage, and power flow conditions at each node. For example, RRCs have implemented systems for making improvements and additions to transmission lines, transformer, and flexible alternating-current transmission systems without government intervention and oversight. The reason that NERC and RRCs have been relatively successful at some self-regulation is because owners and operators understand the interconnected systems better than government bureaucrats, and they prefer to adopt solutions on their own. Industry also prefers self-regulation since government unilateral regulations can often stifle innovation within the industry. NERC highlights the progress self-regulating agencies can make. Unfortunately, when voluntary participants chooses not to implement recommended actions, NERC also highlights the need for a regulating agency to force compliance. Self-regulation is most effective when it is backed by a credible threat of government action.

FERC currently has no direct role in reliability policy and regulation. However, DOE and FERC could take a role in monitoring and enforcing compliance with standards and requirements established by NERC. Past legislation extends authority to

these federal agencies to intervene when NERC and RRC fail to mitigate system disturbances as result of non-compliance.[13]

Other components of the reliability organization structure include private organizations made up of companies and municipalities that own and operate portions of the generation, transmission, and distribution systems. These organizations include: Edison Electric Institute (EEI), American Public Power Association (APPA), National Rural Electric Cooperative Association (RECA), Electric Power Research Institute (EPRI), Canadian Electricity Association (CEA), and the Electric Power Supply Association (EPSA). These organizations help the companies and municipalities share information with each other in a formal setting.

Case Study: NERC

NERC is a non-profit organization that brings together government and industry officials to create standards and policies for energy production and distribution. NERC was formed in 1968 after a massive blackout three years earlier that affected the Northeastern United States and Canada.[14] NERC's primary focus is long-term prevention of system disturbances. A disturbance is defined in the *Guideline for On-line Computer System Performance During Disturbances* as "an event resulting in widespread interruption and characterized by one or more of the following phenomena: the loss of power stability, cascading outages of circuits, abnormal ranges of frequency or voltage or both."[15] NERC is currently undergoing a major transformation and will likely disband or be incorporated into a regulatory agency.

Two key problems exist in the current reliability structure:

- **Lack of coordination** between recently developed infrastructure protection agencies (CIAO and NIPC) and federal agencies (DOE and FERC). This lack of coordination makes it difficult for NERC and industry to continue providing coherent self-regulation policy that is responsive to the regulatory and infrastructure protection-related federal agencies. In some instances, requirements and suggestions from both types of federal agencies flow through NERC to state and local reliability organizations that interact directly with owners and operators.

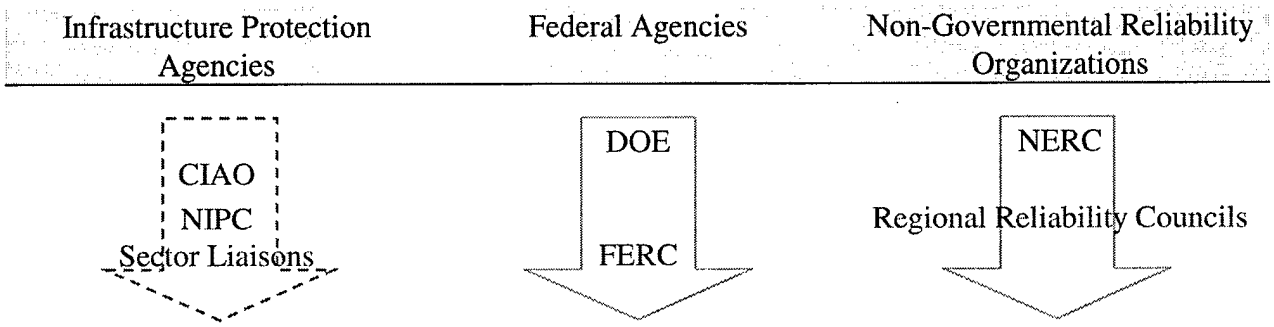
[13] Ibid. p. 6.
[14] www.nerc.com/about/ cited December 17, 1998.
[15] NPCC Document B-12, Guidelines for On-line Computer System Performance. August 7, 1996.

- **Lack of authority to ensure industry compliance** of NERC's standards and requirements on reliability issues. NERC has no regulatory power and cannot legally enforce its decisions through voluntary organizational structure. This lack of necessary authority is the main reason for NERC's demise. Although most industry participants follow NERC's guidelines, a few companies do not, which leads to problems for an interdependent system.

Just as deregulation necessitates new procedures and practices for controlling use of the grid, new practices and procedures also demand new paradigms governing the relationships between DOE, FERC, NIPC, CIAO, and industry. Information sharing continues to be an important part of modifying standards and procedures to improve reliability. The extensive network of industry participants and the federal bureaucracy complicate information sharing. The various layers of reliability regulation are slow to respond to industry concerns. From the government perspective, the primary barrier to information sharing is the reluctance of the private sector to divulge data that may be advantageous to competitors.[16] Self-regulated industry changes in information sharing have the potential for improving overall electric power reliability coordination. However, it may be still be necessary for the government to wield regulatory power to enforce compliance should industry fail to take adequate measures.

[16] Guy Copeland, Speech at Defense Week Conference on Defending Critical Infrastructure, Washington D.C. December 7, 1998.

Current Anatomy of Electric Power Reliability Coordination



This chart shows the coordination of reliability organizations in establishing industry standards and requirements. CIAO and NIPC are new agencies that have yet to affect any changes in industry standards and requirements. The major stovepipes in the current structure occur with federal agencies and infrastructure protection agencies that are segmented from NERC and RRCs. This structure leads to problems in coordinating reliability standards across organizations.

Assessing Power Reliability

Positive Industry Characteristics

To promote assurance, the electric power industry currently exhibits many positive characteristics:

- System operators train on a regular basis with simulations of the grid to learn how to react to potential power outages with a dispatch change.[17]
- System operators take long term precautionary measures by closely monitoring and sometimes advising new system construction and design.[18]
- System controllers refine scheduling requirements, so they can use advance information to plan the settings for the grid days and weeks in advance and, ultimately reduce the possibility of human error.[19]
- Development continues on new controller systems to replace older electromechanical ones, to respond to fluctuations faster, and to govern the flow of current in real time.[20]
- Industry spends much time and energy dealing with human management issues.
- Industry is open-minded about refining policies and procedures in order to reduce vulnerabilities.

Problems in the Electric Power Industry

Despite these positive trends, the electric power industry is still vulnerable and perhaps even more vulnerable today than in the past. According to the Department of Energy, there have been over 1,000 "incidents" against the United States energy infrastructure over the past 15 years with the bulk of those occurring in the electric power industry.[21] These incidents include human error, computer failure, physical accidents, deliberate acts of sabotage, and terrorism. But more importantly, there may be

---

[17] Peter Fox-Penner. Electric Utility Restructuring. Vienna, Va. Public Utility Reports, Inc: 1997. p. 33.
[18] Ibid. p. 29.
[19] Ibid. p. 33.
[20] *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures*, Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office, Washington, DC, July 1998, p. B-43.
[21] Ibid p. B-2.

dangers to the electric power system that remain unknown. Combined, these factors present a hazard to the continued assurance of the industry.

These problems share some common elements; namely, they lead into the vulnerabilities, artificial or inherent, of the industry. Some factors that affect physical vulnerabilities include:

- Physical exposure of power lines
- Readily available information on how to attack power stations, transformers and lines
- Consolidation of much of the physical infrastructure, due to new zoning and regulations
- Increased near-limit peak usage times
- Lack of physical protection spending due to the high cost and low probability of an event, along with the free-rider problem[22]

The electric power industry is very good at protecting against environmental factors that can lead to some power outages, since outages due to tree limbs and human error tend to affect their bottom line. However, there are some issues that are simply too broad for any one company to address on its own:

- Industry is dependent on the fully interconnected SCADA[23] system which uses (open source code) Linux as the Operating System.
- Information and tools are readily available that can delay or deny information.[24]
- Terrorists and hostile states have increased ability to act in the cyber realm.
- Control and security nodes tend to be combined for efficiency and technical reasons.[25]

---

[22] The 'free-rider problem' is when all firms gain benefit from a common area, such as security, but where the contribution of any one firm is insignificant when compared to the whole. Therefore, it is in the best interest of each individual firm not to contribute, but rather free-ride on others' contributions. Many times this leads to inaction.

[23] The Supervisory Control and Data Acquisition (SCADA) serves as the link between control centers and critical equipment. It balances power flows, regulates voltages, and controls frequencies.

[24] There are a plethora of sites like www.digicrime.com, where for free or a fee you can get viruses, trojans, and instruction on information and network denial.

[25] Information security is problematic because it is costly to implement, requires outside expertise, and demands constant revision. Speech at the Kennedy School of Government by Kawika Daguio, "Strategic Information Warfare in the Financial Infrastructure." February 25, 1999.

These factors, together with the problem that there is little delineation of who has responsibility for various parts of the infrastructure, lead to the most potentially damaging threat: a concerted, coordinated attack against the infrastructure in both the physical and information realms at the same time, coupled with near capacity usage. The fact that the industry does not have a coordinated set of standards to deal with threats, vulnerabilities and other problems exacerbates the possibility of broad impact.

General obstacles

Several factors lead to less than optimal investment in assurance and protection. These obstacles inhibit spending and reduce the efficacy of measures that might be taken:

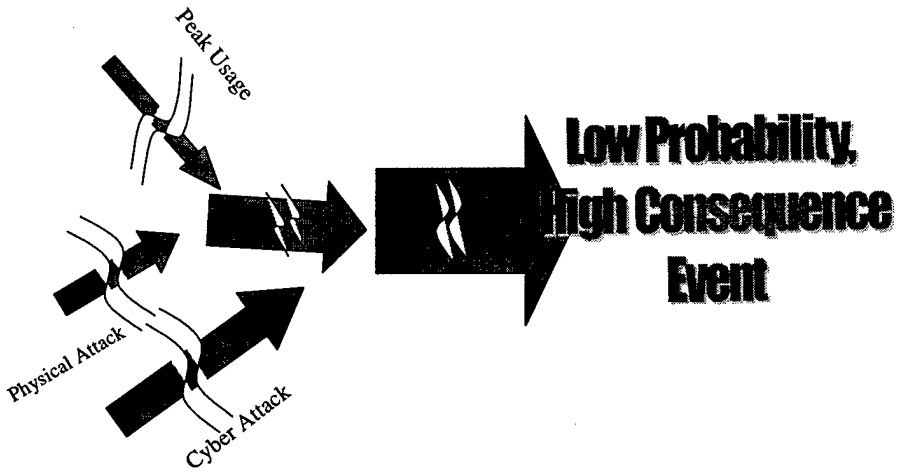
- A more competitive environment augments the industry's high cost/low benefit perception of assurance. As a result, few companies are willing to commit resources to R&D because any benefits accrued must be spread to the entire industry to be effective.
- Imperfect risk assessment information leads to less than optimal levels of spending for addressing vulnerabilities.
- The government at times is unable and unwilling to share existing information, such as specific terrorist attempts thwarted.[26]
- Individual companies fear violating antitrust/collusion laws.
- Industry has reservations about the continuity of government policy, and fear retroactive regulations.
- Department of Energy (DOE) has not made assurance a top priority. According to Dan Adamson, DOE is concerned about electric utility reliability, but has not made it an agency priority due to limited resources and the uncertainty as to who has responsibility for specific pieces of this issue.[27]

[26] This observation comes from several interviews with FBI, DOD, and DOE officials.
[27] Interview with Dan Adamson, DOE. December 7, 1998.

Focus of this study: Three specific vulnerabilities

As discussed above, there are many problems affecting the industry, but they generally lead to several broad categories of vulnerabilities. In order to limit our paper, we narrowed our focus to these three specific vulnerabilities:

- **Physical Terrorism:** an attempt to impair or prevent the propagation of electric power, by attacking exposed, physical infrastructure
- **Cyber Attacks:** an attempt to cause a failure of the communication or control systems of the infrastructure
- **Confluence of Events**: instabilities resulting from a combination of failures and/or attacks on multiple parts of the infrastructure nearly simultaneously



Confluence of Events

This diagram shows how the confluence of several smaller events, each of which may be easily contained in its own right, could be brought together to cause an uncontrollable catastrophe.

Recommendations

Template for Recommendations

Our recommended solutions cross a wide spectrum of options and involve many different entities. In order to present our ideas in a logical, thorough manner, we divide each option into several areas:

- Specific action, including entities involved, anticipated lead actor, and discussion
- Expected benefits of the recommended action
- Obstacles to implementing the recommendation
- Specific problem or vulnerability that the recommendation addresses (physical terrorism, cyber attack, or the confluence of several events nearly simultaneously)

For an example, we applied our template to a public-private partnership (Infragard), see Appendix A.

Recommendations

After examining pertinent literature, interviewing people involved at all levels of the public, private, and nonprofit sectors, and studying some existing models, we developed several recommendations for specific action. These recommendations will help government and industry leaders initiate dialogue leading to actions that will reduce vulnerabilities. Each of our recommendations addresses one or more of the three major vulnerabilities: physical terrorism, cyber attacks, and the confluence of several events occurring nearly simultaneously.

Summary of Recommendations

Recommendation	*Lead Actor*	*Entities Involved*	*Benefits*	*Obstacles*	*Vulnerabilities Addressed*
Establish NAPAC	Government	Private Industry; Government	Command and control center for assurance efforts; Multilevel control; Regulatory power	Funding; Complexity; Industry Resistance	Physical Terrorism; Cyber Attacks; Confluence of Events
Clearly Delineate Responsibility	NAPAC	Private Industry; Government; NAPAC	Improve vertical integration of assurance efforts	Private Industry opposition; Heavy-handed government involvement	Physical Terrorism; Cyber Attacks; Confluence of Events
Implement Red Team Security Testing	NAPAC	Private Industry; Government	Identify existing and new vulnerabilities; Forces constant policy, procedure review	Monitoring; Funding; Security of information	Physical Terrorism; Cyber Attacks
Create an ISAC	Private Industry	Private Industry; Government and NAPAC by invitation	Opens the flow of contacts and information; Addresses 'big picture' issues	Lack of regulatory power to mandate recommendations	Physical Terrorism; Cyber Attacks; Confluence of Events
Create a Modeling and Simulation Center	ISAC	Private Industry	Ability to test scenarios w/o affecting normal operations; Adaptable to changing vulnerabilities	Funding; Credibility; Expertise and Technology	Physical Terrorism; Cyber Attacks; Confluence of Events
Conduct Periodic, Announced Inspections	ISAC	Private Industry; NAPAC	Working inspection environment fosters cooperation and security	Industry opposition; Cost	Physical Terrorism; Cyber Attacks
Legislate Anti-Trust Exemptions	Congress	Private Industry; Government; NGOs; Judicial Branch	Allows private industry to aggregate threat data and solutions to possible vulnerabilities	Congressional and political opposition; Legal issues (consumer protection); Potential for abuse	Physical Terrorism; Cyber Attacks; Confluence of Events

1) Establish the North American Power Assurance Council, NAPAC

Action - Establish an organization responsible for regulating, coordinating and overseeing interdependent reliability aspects of the electric power industry. Overall, the council will evolve from the principles of its predecessor, NERC, which is in the process of dissolving.

Authority Precedent

1988 – The Supreme Court determines that FERC has the authority to force equitable transmission access. Private industry is obligated to honor FERC decisions. Although FERC does not deal with reliability issues, NAPAC could operate under the same rubric with respect to reliability issues.[28]

- **Lead agency** – The federal government will have overall responsibility.
- **Entities Involved** –Government, private industry representatives, and non-governmental members from both the profit and not-for-profit sectors.
- **Discussion**- NAPAC will take the responsibility to coordinate the actions of the many players involved in the assurance of the electric utility infrastructure. More importantly, it will also possess the authority to make binding decisions with the ability to address any entity's failure to comply. The leader of NAPAC should be appointed by the President and confirmed by the Senate, signifying the importance of the position and of the issues the leader will be required to face. Thus, if the industry fails to establish and follow clear assurance procedures on its own, NAPAC will perform the following major functions:

    - Define and implement electric power reliability standards for the entire industry.
    - Ensure compliance with these reliability standards.
    - Serve as the overall reliability command and control element for the system.

Benefits

- NAPAC will provide a command and control center with the ability to oversee and coordinate reliability activities at multiple levels. One organization serving this purpose will allow real-time monitoring of the grid to deal with grid scale instabilities.
- NAPAC will also serve as a centralized institution for the acquisition and dissemination of information critical to other elements within the system. It will act as a conduit of information about threats from the government to industry and about problems from industry to the government.
- This new organization will provide entities with one organization to clarify confusing or nonexistent regulations. Furthermore, NAPAC will have regulatory authority to enforce security-related regulations.

[28] Mississippi Power and Light Co vs. Mississippi, Supreme Court case (487 US 354) 1988.

- If necessary, NAPAC can establish and regulate that private industry take specific measures to reduce both computer and physical security vulnerabilities, and will have its own budget for security measures.

Obstacles

- Congress must establish the regulatory agency and appropriate the necessary funds.
- Industry may oppose the establishment of NAPAC on the grounds that it may be perceived as re-regulation. Again, however, it is important to highlight the fact that NAPAC will replace and improve upon NERC -- an organization that many industry leaders have supported enthusiastically because of its voluntary nature.
- It will be difficult centralizing decision making in an industry that is in the process of comprehensive deregulation.

2) Clearly Delineate Responsibility

Action –NAPAC will delineate specifically who is responsible for assurance of the various parts of the infrastructure and will have the responsibility to oversee that each entity carries out its specific responsibilities. NAPAC will possess the necessary regulatory powers to institute this recommendation. The problem as it currently exists is that no single agency oversees the entire electric power grid. As a result, many entities involved are unsure as to their specific responsibilities.

- **Lead agency** - NAPAC is responsible for defining and implementing electric power reliability standards for the entire industry. They will utilize the existing and highly effective RRCs to disseminate information and regulation. In addition, they will request that higher organizations filter any information or regulation through them.
- **Entities Involved** – NAPAC, private industry, and other federal agencies involved in energy policy or the overall national infrastructure.
- **Discussion** - As the infrastructure exists today, it is unclear which players have responsibility for what pieces of the overall infrastructure reliability. NAPAC must set clear, consistent, and written standards so that all the entities who own, operate, or use the interconnected electric power systems will know what is expected of them. Assigning responsibility would be the first step to holding members accountable for their actions. It is unclear who owns the problem, and no one wants to bear the cost, according to Peter Fox-Penner, a member of the Brattle Group who has written extensively on the problems and issues the industry faces.[29] Clear delineation would improve transparency in the system, leading to increased responsibility by the entities. It is critical that NAPAC apply consequences for noncompliance in a consistent, nondiscriminatory manner.

[29] Interview with Peter Fox-Penner, Brattle Group, December 8, 1998.

Benefits

- The delineation of clear responsibilities would improve vertical integration of assurance measures within the infrastructure.
- NAPAC could hold entities failing to meet their mandated responsibilities accountable for their failure to comply.
- This recommendation will also provide industry with only one central organization for which it can look for clarification of any ambiguous information or regulations concerning reliability.

Obstacles

- Some industry leaders will oppose any attempt by the government to clearly specify actions they must take. Other industry leaders will welcome the transparency for it will allow them to better focus their efforts.
- Perception of heavy-handed government involvement will make private industry less likely to share other information.[30] In order to overcome this obstacle, NAPAC will need to consult industry leaders in delineating responsibility. Industry is much more likely to accept such a recommendation if it feels it played a significant, meaningful role in establishing responsibilities.

3) Implement Red Team Security Testing

Action – Create Red Teams, under the control of NAPAC, trained as a rapid response force to test suspected vulnerable areas and to provide proactive and useful feedback to industry leaders.

- **Lead agency** – NAPAC.
- **Entities Involved** – Private industry, NAPAC.
- **Discussion** – NAPAC would take responsibility to train and oversee a group of Red Teams, which would know the overall system relatively well and a specific vulnerability area extremely well. These teams would conduct tests on selected sites within the electric power industry and provide feedback to both the entities tested and NAPAC. NAPAC would brief CEO's and some high-level managers well in advance on the date and time of the tests as well as the specific areas the Red Teams will attack. Informing industry leadership ahead of time serves two main purposes: 1) allows industry leaders flexibility in jointly scheduling the tests to minimize disruption to necessary day to day activities; 2) provides the opportunity for industry leaders to take necessary precautions to prevent disruptions to real-time functions, preventing a potential confluence of events scenario. More importantly, the tests would be unannounced, surprise inspections for the electric power front-line workers. The Red Teams would

[30] President Clinton's Commission on Critical Infrastructure Protection (PCCIP) noted this "perception of excessive government interference" and recommended that the government balance that perception "against public perceptions of the loss of the civil liberties and the commercial sector's concern about unwarranted limits on its practices and markets" (http://www.ciao.gov/roadmap-b.pdf, p.42.)

provide immediate feedback to all the players involved in the tests. In addition, the Red Teams would be responsible for capturing general lessons learned for submission to the Information Sharing and Analysis Center (ISAC) (discussed later) and NAPAC, and in developing additional testing scenarios.

Benefits

- Identifies vulnerabilities in the actual operating environment. Workers and managers cannot "cram", as they might be able to do for visits to a modeling and simulation center facility.
- Forces private industry to continuously review and update their policies and procedures.
- Identifies those entities that are weak links in the overall system and, more importantly, provides feedback on ways for them to improve security.
- Offers the opportunity to conduct exercises testing computer system and network vulnerabilities.[31]
- Can elucidate specific vulnerabilities that need further attention, as well as illuminating the types of security measures that succeed in thwarting or mitigating such attacks.
- Allows testing of the effects of coordinated cyber and physical attacks, likely highlighting additional vulnerabilities.

Obstacles

- It will be difficult to monitor the Red Teams to ensure consistency and fairness. In order to mitigate this obstacle, NAPAC will work with industry to create and continuously update Red Team standard operating procedures.
- NAPAC will need the necessary funding in its budget to create, train, and support the Red Teams.
- Private industry will likely fight attempts by outside influences to test their systems. One of their greatest fears is that the Red Teams will share specific attack results with industry leaders at the site of the next test. In order to address this obstacle, the Red Teams will only share specific results with the industry company currently being tested and NAPAC. They will be prevented from discussing any specific previous testing results during current security testing.
- It will be difficult to keep upcoming tests confidential.
- There is also danger of Red Team information and techniques falling into terrorist hands. Unfortunately, terrorists will have access to the "general" lessons learned, as they will be published in the ISAC journal. The benefits gained in overall industry security outweigh this valid concern.

[31] For example, "Eligible Receiver" is a DOD exercise series that points out vulnerabilities in the DOD computer system. With DOD personnel successfully "breaking into" their own computer systems, the results showed that deep penetration was possible without immediate detection. As a result of these exercises, DOD completely overhauled its network security protocol.

4) Create an Information Sharing and Analysis Center (ISAC)

Action – Private industry should create an Information Sharing and Analysis Center (ISAC). As discussed in PDD-63, this voluntary organization would gather, analyze, sanitize, and distribute private sector information for the industry. Its primary focus would be on technical information. NAPAC members would participate in the center's activities upon invitation, but private industry clearly has the lead.

- **Lead agency** – Private industry.
- **Entities Involved** – Private industry, federal government, NAPAC, and non-governmental organizations.
- **Discussion** - The idea of a private industry Information Sharing and Analysis Center (ISAC) originates in Presidential Decision Directive 63.[32] No ISACs exist to date despite President Clinton's strong support for the creation of an ISAC in each of the national infrastructures. In this sense, the electric power industry has an opportunity to set a precedent and take the lead for all the country's national infrastructures. The goal is to create a strong, effective partnership between industry owners and operators and the government. External participants will include universities, industry associations, and other non-profit research institutes. The specific mission of the ISAC will be to serve as an information sharing focal point, leading to a better understanding of the infrastructure's threats, vulnerabilities, and interdependencies. Additionally, according to PDD-63, the ISAC would "establish baseline statistics and patterns",[33] act as a clearinghouse for information, publish a monthly newsletter, and serve as a library for historical industry data.

  Why do we need ISACs?

  According to Dr. Jeffrey Hunker, "the fact is, right now, best practices as to how to protect against cyber attacks, and information about real or potential threats, are frequently not shared between companies, and between those in the private sector and public sectors who could act on the knowledge."[34] Doug Perritt, head of the National Infrastructure Protection Center, echoed similar problems from the government end, "the government withholds all kinds of pertinent information that it really has no inherent reason for keeping from private industry."[35] Thus, an ISAC would facilitate better information sharing from both ends.

  Government Tax Incentives for an ISAC

  In order to promote participation in an ISAC, the federal government can use tax incentives. The government should offer tax incentives for companies to participate in the ISAC, based on the idea that the government is actually saving money by not having to force regulation on a resistant

[32] The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. The White Paper. May 22, 1998, p. 9.
[33] Ibid. p. 2.
[34] Dr. Jeffrey Hunker, Director CIAO, Testimony before Congressional Committee, June 11, 1998.
[35] Interview with Mr. Doug Perritt, Deputy Chief, NIPC, December 8, 1998.

industry. In addition, the government, the industry, and the country benefit from the decreased likelihood of an event occurring.

Benefits

- Private industry takes the lead in developing the ISAC, and thus can shape the assurance organization to its specific abilities and needs.
- The concept of an ISAC is supported by the President of the United States as a means of dealing with assurance problems. PDD 63 also recommends federal financial assistance for startup costs.
- ISACs can be used for non-retributional reporting, which has proven useful in dealing with the current Y2K problems.
- Industry is more likely to support options not involving direct government intervention.
- ISACs can deal with problems that are 'bigger' than any individual company, or even section of the industry, and can take a long-term approach to assurance. This ability to combine elements of time, finance, technical feasibility and probabilistic analysis will allow ISACs to flexibly deal with a broad range of problems and vulnerabilities.

Obstacles

- Industry may resist sharing sensitive information in an unproved system. However, NERC currently performs some of these functions, so there is precedent for this sort of information sharing.
- Industry has concerns over liability, anti-trust, and privacy issues.[36]
- Government funding may lead to the government trying to shape or move the ISAC in directions the government considers important.
- Lack of directive power means that any recommendations coming from the ISAC will be completely voluntary. This has been a large issue with NERC because some participants do not comply with its recommendations.

5) Establish an Electric Utility Modeling and Simulation Center (EUMSC)

Action – The ISAC should create a modeling and simulation center allowing industry leaders to conduct exercises aimed at training operators and managers to react effectively in a variety of emergency situations. No simulation center currently allows front-line workers and managers to practice grid level event scenarios without directly affecting real-time operations.

- **Lead agency** – ISAC.
- **Entities Involved** – Private industry.

[36] Mitretek Systems, Inc. A Public Interest Partnership to Implement the Information Sharing and Analysis Center for Critical infrastructure. Washington DC, 20 August 1998.

- **Discussion**- Industry already recognizes the need for the capability to test and train front-line workers and managers on multiple scenarios focused on mitigating vulnerabilities. Specifically, one regional organization, the Northeast Power Coordinating Council (NPCC), has already developed simulation testing for industry people within its boundaries. EUMSC could emulate certain aspects of both the NPCC model and other precise simulation models. The NPCC model is encouraging in that the technology exists specifically with respect to the electric power industry. The NPCC simulation model allows trainers to conduct a specific scenario focused on one specific vulnerability and then turn around and conduct a completely different scenario focusing on different vulnerabilities all within in a relatively short period of time. Some inviting aspects of other models include precise, clear standard procedures on effective ways to discuss lessons learned, illustrate possible techniques to improve the deficiencies, and then retrain in problem areas.

  Industry Precedent

  The task force on energy management technology for the Northeast Power Coordinating Council (NPCC) has recommended the establishment of simulation testing for their region.[37] The challenge for EUMSC will be to build on this NPCC example and create a comprehensive simulation center.

  The envisioned environment of EUMSC will be one focused on learning from mistakes and getting better each training day. The most critical component of the training is the daily after action reviews (AARs) where the simulation managers lead a discussion of what went wrong and why. It will be critical for private industry to play a major role providing the technical expertise in the development of the many scenarios. In addition, industry leaders will set the tone on whether the training is perceived as constructive and able to reduce vulnerabilities or a check-the-block exercise. Finally, and of fundamental importance, is the fact that EUMSC will allow for training on both low and high probability vulnerabilities. **As a result, even if industry is skeptical of training on low probability scenarios, they are likely to accept the opportunity to improve best practices in areas with a higher probability of problems, such as human resource management, where they have been consistently strong in the past.**

Key elements of the simulation center:

- The ISAC would capture systematic lessons learned and publish a journal available to everyone involved in the protection of the electric utility infrastructure.
- EUMSC would certify attendees who successfully complete the training courses. The ISAC would not need to initially require that all electric power workers be certified. Initial involvement should be voluntary.
- The center would provide a forum to test many scenarios, without the fear of interrupting normal operations or initiating real world problems within the electric power industry.

[37] NPCC (Northeast Power Coordinating Council) Document B-12, p. 4.

Benefits

- Private industry will be more likely to support changes where it has the lead.
- The center will have the ability to adapt training to changing vulnerabilities. This adaptability component allows the simulation center to meet President Clinton's concerns that "as technology and the nature of threats to our critical infrastructure will continue to change rapidly, so must our protective measures and responses be robustly adaptive."[38]
- Another benefit is the capability to test scenarios without interrupting normal operations.
- The NPCC model can serve as a basic starting point for creating a grid scale model.
- This proposal addresses vulnerabilities at the lowest level – front-line operators and managers.
- By assisting with the funding, the government shows its willingness to serve as a partner with a genuine interest in taking positive, constructive steps in reducing vulnerabilities.
- The center has the capability to incorporate the Red Team lessons learned into new scenarios.
- The scenarios can demonstrate to the operators powerful examples of existing computer vulnerabilities and the means of mitigating consequences which they may not have considered previously.
- The focus of the center allows practice and training in the types of security measures that succeed in thwarting or mitigating attacks.
- The flexibility of the center allows operators to see the effects of coordinated cyber and physical attacks, and to practice mitigating or eliminating these additional vulnerabilities.

Obstacles

- Initial outlays for buildings and equipment will be significant. Private industry will be expected to provide some funding because they will be taking the lead.
- It will take several years for the simulation center to establish credibility.
- Private industry will not necessarily want to share information with its competitors, leading to less than optimal scenarios.
- There are technological challenges to building a realistic simulation center. The NPCC simulation model is only based on a specific, limited region. That model does offer high expectations that it could serve as the foundation for a larger scale, national model.
- The "free-rider problem" causes many private industry companies to want to hold off funding until they know the modeling and simulation center will produce improvements worth the effort and resources required (at the expense of those who choose to participate from the beginning).

[38] The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. The White Paper. May 22, 1998, p.3.

6) Conduct Announced, Open Security Visits

Action – The ISAC in conjunction with NAPAC will conduct open, announced inspections of the entities involved in the electric power infrastructure. The ISAC will establish inspection criteria and industry-wide standards through consensus. The announced, working inspections are much different from the Red Team activity, which will focus on front-line worker and manager reaction to security tests or breaches. The inspections will allow both NAPAC officials and industry personnel to discuss deficiencies and methods to improve them.

- **Lead agency** – ISAC.
- **Entities Involved** – Industry/ISAC, NAPAC.
- **Discussion**- This recommendation stems from the belief that the American public, government officials, and even some in the industry itself do not clearly understand the significance of the three vulnerabilities discussed in this paper. In addition, they may not fully understand that the infrastructure is vital to our overall national interests. The ISAC's primary mission would be to visit all the sites involved in the infrastructure and to rate each site on the "security" of its systems. These announced visits would be working inspections in which ISAC inspectors share lessons learned. Importantly, the environment will be one of joint learning, cooperation, and dialogue on improving current policies and procedures. As such, ISAC inspectors would offer assistance and expertise to correct deficiencies immediately where possible and, more importantly, would record examples of effective "best practices" to be shared with other industry leaders. The ISAC will also share results with NAPAC, which benefits from a better overall understanding of infrastructure reliability issues.

  What should be done with the results?

  1) The ratings should be confidentially held by both the ISAC and NAPAC. Sites "failing" the inspection would be given a reasonable amount of time to demonstrate that they had corrected the deficiencies identified in the survey. Government and industry leaders will have to agree on the definition of a "secure" system; industry will play a key role here. **[Recommended Action]**

  2) Another option put forth by Joseph Nye, Dean of Harvard's JFK School of Government, would be for the government to share the results with insurance companies. The insurance industry would then realize that private industry is accepting more risk than earlier understood. In response, insurance companies would raise insurance rates forcing electric utility companies to take additional measures to "prove" to the insurance companies that they have taken all prudent measures to minimize risk.[39] Through this method, the government could get the

[39] Interview with Joseph Nye, Dean of Harvard's John F. Kennedy School of Government. Cambridge, MA., December 16, 1998.

industry to increase protection of its systems without becoming directly involved. [**Not Recommended**]

Benefits

- Keeping the results of the inspection confidential would support the conclusion that the government is more concerned with reducing vulnerabilities than trying to publicly blame specific industry entities. In other words, it will serve to build trust and positive communication.
- Industry gets a relatively "free" outside look including specific, positive advice on potential ways to improve existing policies and procedures.
- Results serve as a foundation for both the ISAC and NAPAC in determining where to focus security efforts.
- Working inspections create an environment of cooperation and partnership between NAPAC and private industry; a constructive approach to improving security and assurance.
- NAPAC will possess the necessary regulatory authority to require corrections and take action against industry entities failing to meet minimum standards. While regulation is not the preferred method, it is important that the option exists.

Obstacles

- Private industry and the government will need to agree on "acceptable" standards for security and vulnerability reduction as well as "reasonable" periods in which the ISAC and NAPAC require deficiencies be corrected.
- Some companies, which believe they have been treated unfairly by the inspection system, will pursue political (their Congressman) and legal (the courts) avenues to prevent NAPAC from mandating specific corrections/actions.
- The private industry members making up the ISAC inspection team could leak the results back to their parent company.

7) Legislate Anti-Trust Exemptions

Action - Congress should pass legislation granting anti-trust exemptions to electric power companies allowing them to share certain security information as well as details of different approaches for reducing existing vulnerabilities without fear of legal ramifications. According to an analysis of anti-trust issues by members of the Hunton & Williams Law Firm, both governmental and industry leaders are concerned that reliability discussions between competitors or industry and government sometimes involve "commercially valuable information on market conditions, such as unit availability and outages, load projection, and current and future transmission capability."[40] It is this gray area which makes some industry leaders hesitant to share information. Further, private entities, such as NERC, have no special status under the Sherman Act and must comply with all anti-trust laws. In order to avoid conflicting

[40] William Young and Gregory Kinzleman of the Hutton & Williams Law Firm, Washington, DC, undated.

federal mandates, the courts often rule that federal agency regulations, such as the ones we propose under NAPAC, preempt the Sherman Act. In other words, Congress is much more likely to grant an exemption where a federal regulatory agency is involved, further building a case for the need of NAPAC.

- **Lead agency** – Congress would grant the exemptions through specific legislation.
- **Entities Involved** – Private industry, the government, NAPAC, and non-government agencies. Use of Justice Department officials and other legal experts will be essential in order to minimize the possibility of future lawsuits.
- **Discussion-** Section 1 of the Sherman Act prohibits any "contract, combination or conspiracy" between two or more entities to restrain competition.[41] Thus, any agreement between actual or potential competitors, including discussions on ways to reduce anticipated threats and existing vulnerabilities, is potentially subject to the Sherman Act. In general, however, sharing information in order to establish industry standards is not illegal. The fear is that in discussing reliability issues, market and price data may need to be addressed. The courts analyze both the "purpose" and "effects" of such agreements in determining if anti-trust laws were violated.

Benefits

- Legislation could allow private industry to aggregate threat and vulnerability data, improving the range of possible solutions and giving the simulation center additional scenarios to test and train.
- Positive, non-heavy-handed steps by the government will show it is genuinely interested in helping to reduce industry vulnerabilities and increasing trust.
- Private industry would likely support the move.
- Anti-trust exemptions would likely lead to increased dialogue on specific vulnerabilities and "stories" of what has gone wrong in the past and how a specific electric power company overcame the problem.

Obstacles

- Some representatives in Congress will fear 1) the precedent that exemptions could create since other industries may follow with similar requests, 2) potential industry abuses of actually sharing information for competitive advantage purposes.
- Consumer protection groups may lobby congressman to oppose the legislation. In order to overcome these obstacles, it will be necessary for the electric power industry to counter with a lobbying effort of its own. Industry personnel will need to contact their representatives in large numbers.

[41] Sherman Act 15 U.S.C.

Conclusion

Infrastructure assurance in the electric power industry is vital to our national interests. Assurance cannot be achieved quickly, cheaply, or easily, but the problems leading to limited assurance must be addressed. Protection of the electric power industry's infrastructure is vital because of its direct impact on so many other national critical infrastructures. Upon examination of the vulnerabilities facing the power industry today, the industry deserves tremendous credit for taking the necessary measures to protect against catastrophic failures and to minimize the impact of accidents. Indeed, it is mostly due to their focus, time, resources, and efforts that the American public has confidence in the electric power industry and its ability to deliver electricity. Still, the electric power industry is currently evolving through a major transitional period. This transition has created new opportunities and efficiencies, but also brings with it new vulnerabilities, such as greater susceptibility to physical terrorism and cyber attack.

The best set of solutions will involve private industry, the government, non-governmental organizations, and other third party actors. The most pressing requirement is for action to begin immediately. As General George Patton said, "a good plan executed today is better than a perfect plan next week." All participants must work together now to insure that this vital infrastructure remains stable and secure, providing reliable power to our nation for years to come.

Appendix A: Case Study

Infragard

Action - The FBI created Infragard in 1996 to coordinate and manage investigations involving computer crimes and national security and terrorist cyber threats to the national infrastructure.

- **Lead agency** – The Federal Bureau of Investigation (FBI), Office of the National Infrastructure Protection Center (NIPC).
- **Entities Involved** – Infragard is an alliance between both the public and private sectors including the FBI, other government agencies, the business community, and academic institutions.
- **Discussion** -The FBI established a pilot program in Cleveland with the hope of developing a free flow of information as well as to coordinate responses to attacks on the national infrastructure. Infragard has two main components: an alert network and a website to serve as a focal point for information sharing. The many, different players report intrusions to the FBI in two, separate, encrypted emails: a detailed description for the FBI to analyze in depth and a sanitized version devoid of all agency-specific material to be shared with all other players in the Infragard system.[42]

Benefits

- Ability to identify several players from both the public and private sectors; their goal is to keep membership to less than 150 people.
- Conducted groundwork meetings as a foundation upon which to build future, more substantive efforts.

Obstacles

- Actual output has been minimal because of the painfully slow process.
- No clear delineation of member responsibilities.
- Development of concise rules for information sharing still not accomplished.
- Private firms are extremely concerned that shared information could jeopardize their competitiveness; they desire sanitized versions for overall distribution.

Vulnerability Addressed

- Terrorist cyber attacks.

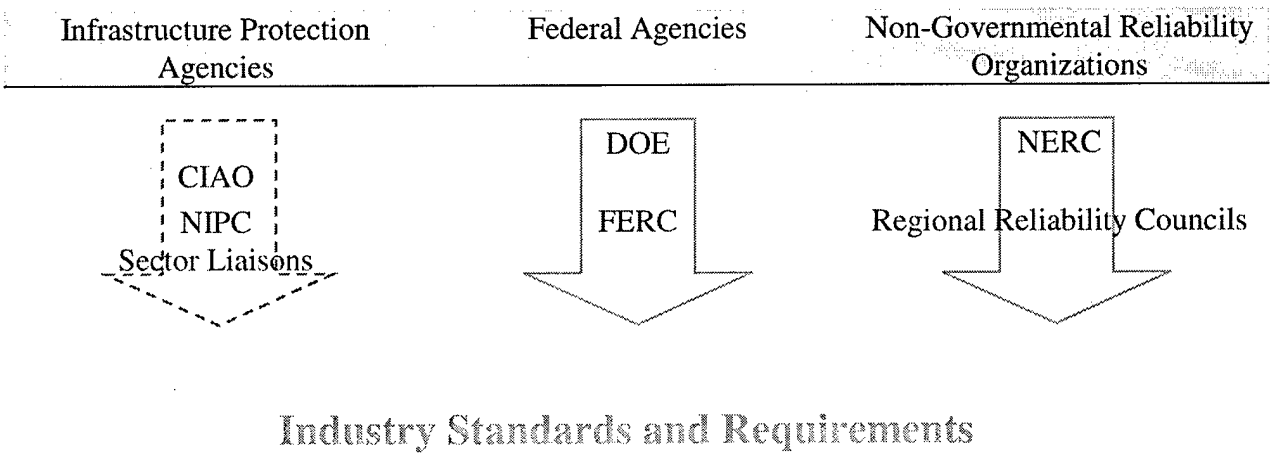
Overall, Infragard is still in the early stages. The benefits and obstacles to date, however, do provide concrete examples of the issues we must address in each of our recommended actions.

---

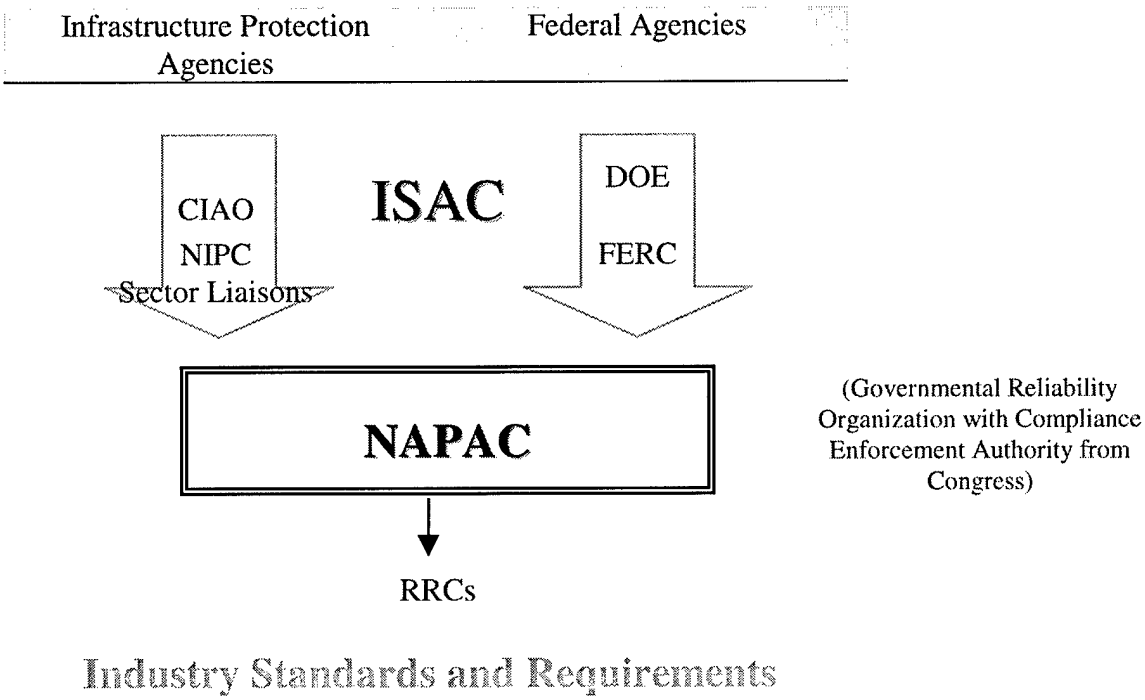
[42] http://www.fbi.gov/nipc/nipcfaq.htm, section E-2.

Appendix B

Current Anatomy of Electric Power Reliability Coordination



Proposed Anatomy of Electric Power Reliability Coordination



Interviews

Joe Nye, Dean of the Kennedy School of Government, Harvard University
Interviewed December 10, 1998 by Troy Perry

From 1977 to 1979, Dean Nye served as Deputy to the Under Secretary of State for Security Assistance, Science and Technology and chaired the National Security Council Group on Nonproliferation of Nuclear Weapons. In recognition of his service, he received the highest Department of State commendation, the Distinguished Honor Award. In 1993 and 1994, he was chairman of the National Intelligence Council, which coordinates intelligence estimates for the President.

Michael Vatis, Federal Bureau of Investigation (FBI)
Interviewed December 7, 1998 by Dan Feliz

Michael Vatis serves as Chief of the National Infrastructure Protection Center (NIPC) that was established in February 1998. The NIPC's mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. Michael Vatis is a Magna Cum Laude graduate of Princeton University and Harvard Law School.

Doug Perritt, FBI
Interviewed December 8, 1998 by Max Bremer and Troy Perry

Mr. Perritt works at the FBI headquarters and has been actively involved in addressing critical infrastructure protection issues. Mr. Perritt is now Deputy Director of NIPC.

Richard Clarke, National Security Council
Interviewed December 7, 1998 by Dan Feliz

President Clinton appointed Richard Clarke as the first National Coordinator for Security, Infrastructure Protection, and Counter-terrorism in May 1998. As National Coordinator, he reports to the President through the National Security Advisor and, when the NSC Principals Committee meets on security issues, he serves as a full member of that Cabinet-level committee. In the Reagan Administration, Mr. Clarke was the Deputy Assistant Secretary of State for Intelligence. In the Bush Administration, he was the Assistant Secretary of State for Politico-Military Affairs. In 1992, Mr. Clarke joined the National Security Council staff. Among the issues he has handled there, as Special Assistant to the President for Global Affairs, are the reform and reduction in the cost of UN peacekeeping, the restoration of democracy in Haiti, Persian Gulf security, and international crime control. He has served as chairman of the interagency counter-terrorism committee since 1992.

Jeffery Hunker, Critical Infrastructure Assurance Office
Interviewed December 7, 1998 by Dan Feliz

Dr. Jeffrey A. Hunker is Director of the Critical Infrastructure Assurance Office. As Director, Mr. Hunker will be responsible for bringing together an integrated national plan for addressing physical and cyber threats to the nation's communications and electronic systems, transportation, energy, banking and financial, health and medical services, water supply, and key government services. Prior to joining the office, he served as Deputy Assistant to the Secretary of Commerce, where his responsibilities included issues relating to overall economic policy development and initiatives, the integration of economic, energy, and environmental issues, China and other developing countries, and representing the Administration with key constituencies.

Jeff Smith, American Bar Association
Interviewed December 8, 1998 by Troy Perry

Jeff Smith is a member of the Standing Committee on Law and National Security for the American Bar Association. The Standing Committee on Law and National Security, founded in 1962, conducts studies, sponsors programs and conferences, and administers groups on law and national security related issues. In 1993, Mr. Smith served as the military advisor to President-elect Clinton on the Presidential Transition Team.

Bill Hogan, Professor Harvard University
Interviewed February 12, 1999 by Dan Feliz

Professor Hogan is Research Director of the Harvard Electricity Policy Group, which is exploring the issues involved in the transition to a more competitive electricity market. He was a member of the faculty of Stanford University where he founded the Energy Modeling Forum, and he is a Past President of the International Association for Energy Economics (IAEE). He has held positions dealing with energy policy analysis in the Federal Energy Administration, including that of Deputy Assistant Administrator for Data and Analysis. Professor Hogan is a Senior Advisor to Putnam, Hayes & Bartlett, Inc. He is involved in research and consulting activities including major energy industry restructuring, network pricing and access issues, and privatization in several countries.

Phillip Sharp, Professor Harvard University
Interviewed February 15, 1999 by Max Bremer

Since February, 1995, Philip Sharp has been a Lecturer in Public Policy at the John F. Kennedy School of Government, Harvard University. He is associated with the Harvard Electricity Policy Group and is teaching a course on restructuring the electric utility industry. From July, 1995, until February, 1998, he was Director of Harvard's Institute of Politics. He chairs the Electric System Reliability Task Force for the Secretary of Energy and is a member of the Secretary's Advisory Board. He also serves as Vice Chair

of the Energy Board of the Keystone Center and as a member of the boards of directors of the Energy Foundation and the Cinergy Corporation. Sharp was a ten-term member of Congress (1975-1995), representing the second district of Indiana. He was a member of the House Energy and Commerce Committee and the Interior Committee. He chaired the Subcommittee on Fossil and Synthetic Fuels (l981-1986) and the Energy and Power Subcommittee (1987-1995).

Dr. Peter Fox-Penner, Brattle Group
Interviewed December 8, 1998 by Max Bremer

Dr. Fox-Penner is an economist with an engineering background and 20 years experience in regulated industries. He has authored numerous publications and books, spoken at conferences, and directed several complex research efforts. His expertise on a broad range of energy and environmental topics includes electric utility restructuring, performance-based and price cap deregulation, retail utility strategic and economic issues. He has served as senior advisor to the White House Office of Science and Technology Policy and as assistant to the Deputy Secretary of Energy.

General Thomas Marsh (USAF Ret.)
Interviewed December 8, 1998 by Dan Feliz

General Thomas Marsh (USAF-Ret.) is chairman of the President's Commission on Critical Infrastructure Protection. As a former commander of the Air Force Systems Command, General Marsh served as the first chairman of Thiokol Corporation and is currently the chairman of the board of CAE Electronics, Inc. and Converse Government Systems Corporation. The Commission's mandate involves combining governmental and private sector expertise to advise the President on a strategy for protecting and assuring the continued operation of critical infrastructures.

Mr. Fred Herr, National Communication System
Interviewed November 5, 1998 by Max Bremer

Mr. Fred Herr is the Chief, Customer Service and Information Assurance Division (N5), National Communication System.

Mr. John Howell, Compliance Chain Ltd.
Interviewed December 7, 1998 by Max Bremer

Mr. John Howell is the Director of Compliance Chain Ltd. and an advisor to ICC Commercial Crime Services.

Mr. Dan Adamson, Department of Energy
Interviewed December 7, 1998 by Troy Perry

Mr. Dan Adamson is the Deputy Assistant Secretary of Energy for Utility Technologies.

Bibliography

Clark, Richard A. National Coordinator, Security, Infrastructure Protection & Counter-Terrorism, National Security Council. Speech given at the Defense Week 19th Annual Conference on Defending National Critical Infrastructure. Keynote Address. December 7, 1998.

Clinton, William J. Memorandum to the Secretary of Energy as reported in the Critical Infrastructure Assurance Office Report, p. B-2. July 3, 1996.

Copeland, Guy, Vice President, Information Infrastructure Advisory Programs. Speech given at the Defense Week 19th Annual Conference on Defending National Critical Infrastructure. Conclusions and Predictions. December 8, 1998.

Daguio, Kawika, lecture on Strategic Information Warfare in the Financial Infrastructure. Kennedy School of Government, Harvard University, Cambridge MA, February 25, 1999.

Davis, John C. Director of National Computer Security Center, NSA. Speech given at the Defense Week 19th Annual Conference on Defending National Critical Infrastructure. Research and Development Agenda for Critical Infrastructure Protection Technologies. December 8, 1998.

The Department of Energy. The Changing Structure of Electric Power. Washington DC, 1999.

Federal Bureau of Investigation. Infragard Section E-2 <http:www.fbi.gov/nipc/nipcfaq.htm> (cited February 1, 1999).

Fox-Penner, Peter. Electric Utility Restructuring. Vienna, Virginia; Public Utilities Report, Inc., 1997.

Hoffman, Steve. "Enhancing Power Grid Reliability." Electric Power Reliability Journal. November/December, 1996.

Hunker, Jeffrey A. Director, Critical Infrastructure Assurance Office. Testimony before the 105th Congress, June 11, 1998.

Hunker, Jeffrey A. Director, Critical Infrastructure Assurance Office. Speech given at the Defense Week 19th Annual Conference on Defending National Critical Infrastructure. Status Report on National Infrastructure Assurance Plan. December 7, 1998.

Mitretek Systems Inc. and the Institute for the Study of Terrorism and Political Violence. A Public Interest Partnership to Implement the Information Sharing and Analysis Center for Critical Infrastructure. Washington DC, 20 August 1998.

National Security Telecommunications Advisory Committee (NSTAC), Information Assurance Task Force. Electric Power Risk Assessment. Washington DC, 1998.

North American Electric Utility Reliability Council. NERC Mission. <http://www.nerc.com/about> (cited January 12, 1999).

North American Reliability Organization. NAERO Mission. <http://www.naero.org> (cited January 15, 1999).

Northeast Power Coordinating Council. Guidelines for On-line Computer System Performance During Disturbances (Document B-12). Revised August 7, 1996.

Office of the President. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. May 22, 1998.

Perritt, Doug, Deputy Chief, National Infrastructure Protection Center. Speech given at the Defense Week 19th Annual Conference on Defending National Critical Infrastructure. Information Sharing & Analysis Center (ISACs). December 7, 1998.

President's Commission on Critical Infrastructure Protection. PCCIP Report: Critical Foundations. Washington DC, October 1997.

Security Process Task Force. Final Report to the NERC Engineering Committee and Operating Committee. February 27, 1996.

Sen, P.C. Principles of Electric Machines and Power Electronics. New York: Wiley and Sons. 1989.

Serabian, John, Central Intelligence Agency. Speech given at the Defense Week 19th Annual Conference on Defending National Critical Infrastructure. Interagency Implementation Plans & Program Requirements for Critical Infrastructure Protection under PDD 63. December 7, 1998.

Tipler, Paul. Physics for the Scientists and Engineers. Third edition. New York: Worth Publishing, 1991.

Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office. Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures. July 1998.

United States Department of Energy, Secretary of Energy Advisory Board. Maintaining Reliability in Competitive U.S. Electricity Industry-The Final Report of the Task Force on the Electric System Reliability. September 29, 1998.

Young, William F. and Gregory Kinzelman. Regional Reliability: The Potential For Conflict Between Cooperation and Competition. Hunton & Williams Law Firm private working paper, Washington, DC.

Acknowledgements

Major contributors to this paper include:

Mitretek Systems Inc. - our client for this Policy Analysis Exercise. Mitretek is a non-profit company that develops science and technology solutions underlying public policy problems. Mitretek provided the funding and direction for the research and analysis we conducted, as well as feedback on many drafts and ideas. Principal participants from Mitretek include: Robert Clerman, David Allen, Chuck Howell, Willard Fraize, Steve Lipner and William Agresti. Without their heroic and ever tolerant efforts, this product would never have come to fruition.

Dr. John White. Our advisor, who read, re-read and provided much feedback on a series of draft copies.

Marie Danziger, KSG communications program. Marie provided invaluable feedback on how to improve readability, coherence and packaging of our PAE.

Kalypso Nicolaidis, and Dorothy Zinberg, our PAC seminar leaders.

The many people who took time out of their busy schedules to give interviews or answer our questions about the assurance of the electric power industry.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	17.Feb.00	MAJOR REPORT

4. TITLE AND SUBTITLE
CRITICAL INFRASTRUCTURE ASSURANCE: ELECTRIC POWER RELIABILITY

5. FUNDING NUMBERS

6. AUTHOR(S)
1ST LT BREMER MAXIMILIAN K

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
HARVARD UNIVERSITY

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
THE DEPARTMENT OF THE AIR FORCE
AFIT/CIA, BLDG 125
2950 P STREET
WPAFB OH 45433

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
FY00-70

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited distribution
In Accordance With AFI 35-205/AFIT Sup 1

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS

15. NUMBER OF PAGES
43

16. PRICE CODE

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