National Infrastructure Advisory Council

A Framework for Establishing Critical Infrastructure Resilience Goals

Final Report and Recommendations by the Council

October 19, 2010

Alfred R. Berkeley III
Working Group Co-Chair
Chairman
Pipeline Trading Systems LLC

Mike Wallace
Working Group Co-Chair
Vice Chairman and COO, Constellation Energy; Chairman, UniStar Nuclear Energy; Chairman, Constellation Energy Nuclear Group

Table of Contents

Acknowledgements

Working Group Members

Al Berkeley (Co-Chair), Chairman, Pipeline Trading Systems LLC (former Vice Chairman, The NASDAQ Stock Market, Inc.)

Mike Wallace (Co-Chair), Vice Chairman and COO, Constellation Energy; Chairman, UniStar Nuclear Energy; Chairman, Constellation Energy Nuclear Group

Study Group Members

Michael Assante, former V.P. and Chief Security Officer, North American Electric Reliability Corporation

William Ball, Executive V.P. and Chief Transmission Officer, Southern Company

Terry Boston, President and CEO, PJM Interconnection

A. Christopher Burton, Senior V.P.—Gas & Electric Operations & Planning, Baltimore Gas and Electric Company

Gerry Cauley, President and CEO, North American Electric Reliability Corporation

Jeff Dagle, Chief Electrical Engineer, Pacific Northwest National Laboratory

Ken Daly, President and CEO, National Association of Corporate Directors

Kenneth DeFontes, President and CEO, Baltimore Gas and Electric Company

Jose Delgado, former President and CEO, American Transmission Company

Mark Engels, IT Risk Management, Dominion Resource Services

Ed Goetz, Executive Director—Corporate and Information Security, Constellation Energy

Scot Hathaway, V.P.—Transmission, Dominion Virginia Power

Robin Holliday, Joint Operations and Analysis Program Area Manager, Johns Hopkins University Applied Physics Laboratory

Paul Koonce, CEO, Dominion Virginia Power

Rob Manning, Executive V.P.—Power System Operations, Tennessee Valley Authority

Bill Muston, Manager—Research & Development, Oncor Electric Delivery Company LLC

Debra van Opstal, Senior Fellow—Resilience Policy, Center for National Policy

Dan Sadler, Supervisor—Business Continuity, Constellation Energy

Other Contributors

Don Benjamin, Executive Director, North American Transmission Forum

Stephen Flynn, President, Center for National Policy

Al Fohrer, CEO, Southern California Edison

Gary Fulks, General Manager, Sho-Me Power Electric Cooperative

Jeff Gaynor, Founder, American Resilience LLC

Paul Murphy, President and CEO, Independent Electricity System Operator

Vijay M. Nilekani, Senior Project Manager—Security, Nuclear Energy Institute

Susan Perkins-Grew, Director—Emergency Preparedness, Nuclear Energy Institute

Jack W. Roe, Director—Security Integration and Coordination, Nuclear Energy Institute

Mark Weatherford, V.P. and Chief Security Officer, North American Electric Reliability Corporation

BGE Stress Test Participants

Daniel Blaydon, Engineer III—Substation Engineering & Standards, Baltimore Gas and Electric Company
Mel Blizzard, Director—Security Operations Support, Constellation Energy
John Borkoski, Director—Gas & Electric Business Management, Baltimore Gas and Electric Company
Stephen Boutilier, Engineering Consultant—System Analysis & Support, Baltimore Gas and Electric Company
A. Christopher Burton, Senior V.P.—Gas & Electric Operations & Planning, Baltimore Gas and Electric Company
Ed Carmen, Manager—Transmission System Operations, Baltimore Gas and Electric Company
Andy Dodge, V.P.—Electric System Operations & Planning, Baltimore Gas and Electric Company
Ed Goetz, Executive Director—Corporate and Information Security, Constellation Energy
John Houston, V.P.—Transmission Substation Operations, CenterPoint Energy
Charles Matassa, Principal Engineer—Transmission Planning, Baltimore Gas and Electric Company
Robert May, Sr. Engineer—Transmission Engineering, Design & Standards, Baltimore Gas and Electric Company
Sam Modico, Engineer II—Gas Engineering & Standards, Baltimore Gas and Electric Company
John Moraski, Director—Reliability & Compliance Assurance, Baltimore Gas and Electric Company
Scott Prochazka, Senior V.P.—Electric Operations, CenterPoint Energy
Dan Sadler, Supervisor—Business Continuity, Constellation Energy
Dave Souder, Manager Operations Planning, PJM Interconnection
Eric Yeh, Engineer III—TSO Procedures & Training, Baltimore Gas and Electric Company

CEO Roundtable Participants

Mel Blizzard, Director—Security Operations Support, Constellation Energy
A. Christopher Burton, Senior V.P.—Gas & Electric Operations & Planning, Baltimore Gas and Electric Company
Bill Gausman, Senior V.P.—Asset Management, Pepco
Ed Goetz, Executive Director—Corporate and Information Security, Constellation Energy
Michele Guido, Business Assurance Principal, Southern Company
Keith Hardy, V.P.—Distribution, Florida Power and Light Company
Mary Heger, V.P.—Information Technology, Ameren
Shane Hilton, General Manager—Retail Operations, Cleco Power, LLC
John Houston, V.P.—Transmission Substation Operations, CenterPoint Energy
Rob Manning, Executive V.P.—Power System Operations, Tennessee Valley Authority (TVA)
John McAvoy, Senior V.P.—ConEdison
John Procario, Chairman, President, and CEO, American Transmission Company
Scott Prochazka, Senior V.P.—Electric Operations, CenterPoint Energy
Ron Ragains, V.P.—Electric Transmission, Northern Indiana Public Service Company
Joe Rigby, CEO, Pepco Holding Company
Dan Sadler, Supervisor—Business Continuity, Constellation Energy
Jim Turner, Group Executive and President and CEO—U.S. Franchised Electric and Gas, Duke Energy
Mike Wallace (Co-Chair), Vice Chairman and COO, Constellation Energy; Chairman, UniStar Nuclear Energy; Chairman, Constellation Energy Nuclear Group

Support Staff

Jack Eisenhauer, Nexight Group LLC
Martin Lasater, Energetics Incorporated
Jennifer Rinaldi, Energetics Incorporated
Marc Sigrist, Energetics Incorporated
Lindsay Kishter, Nexight Group LLC
Robert Briggs, SRA International
Melissa Hill, SRA International
Patricia Philogene, SRA International

Executive Summary

Our nation faces an increasingly complex set of risks that are interwoven into all facets of our businesses, infrastructures, and communities. The threat of hurricanes, financial instability, pandemics, cyber crime, social unrest, terrorism, and other disruptive events that flow from our participation in a global economy has become a part of our everyday lives. While we continue to work toward a safer and more secure world, the reality is that we must address emerging risks with diligence, commitment, and the understanding that we cannot reroute hurricanes, intercept every cyber attack, or prevent every disruption. President Obama put it succinctly: *"To succeed, we must face the world as it is."*

Critical infrastructure risks pose a special problem for the country. The companies that own these infrastructures operate in competitive and regulated environments and must balance risk, investment, and cost to customers. Although they have a deeply ingrained sense of responsibility to their customers and shareholders, it is neither practical nor possible to safeguard infrastructures from all hazards. For the government, the continuity of these infrastructures—and electric power in particular—is critical to many of its fundamental missions: economic stability and growth, national security, public safety, and quality of life.

Resilience provides the bridge between the possible and the ideal. The National Infrastructure Advisory Council (NIAC or Council) considers resilience to be a fundamental strategy that makes our businesses stronger, our communities better prepared, and our nation more secure. It is often the most flexible and cost-effective strategy to ensure continuity of services and functions and to minimize the impact of disruptions. The *National Security Strategy*, released by the White House in May 2010, recognizes "*the fundamental connection between our national security, our national competitiveness, resilience, and moral example."*

The Council's 2009 report on *Critical Infrastructure Resilience* provided a common definition of resilience but recognized that each sector applies resilience strategies and practices differently. The Council encouraged government to provide each critical infrastructure sector maximum flexibility to develop and adopt resilience strategies that match their operating model, asset base, and risk profile. By doing so, the government policies and programs intended to improve infrastructure resilience can be tailored to the special needs of each sector to achieve maximum results. In this vein, with the support of the Under Secretary for the National Protection and Programs Directorate at the U.S. Department of Homeland Security (DHS) given on behalf of the Secretary of DHS, the Council decided to conduct a study to describe and clarify sector-specific resilience strategies and practices, and how they can serve as the basis for setting sector-specific resilience goals. The Council is using a case study approach of selected sectors to accomplish this request. This document contains the first case studies of the electricity and nuclear sectors and proposes a framework for setting resilience goals within all critical infrastructure sectors.

Scope and Approach

The Council believes that it is the purview of individual companies and sector-wide organizations and institutions to set resilience goals; as such, we did not set goals in this study. Instead, we sought to understand how the NIAC definition of resilience manifests within specific sectors in order to outline a process by which sector goals can be developed and tested.

The electricity sector became the primary focus of these case studies because the nuclear sector had already undergone the voluntary and extensive Comprehensive Review process with the DHS, aimed at improving protection and resilience at nuclear facilities. The Council drew upon the approach used for

the Comprehensive Reviews to design the electricity case study and documented the nuclear experience through discussions with the Nuclear Energy Institute.

The case study process included three important features:

- To conduct the case study, the Council formed a **Study Group that included 14 CEOs and senior executives** who possessed a comprehensive knowledge of power system operations and business priorities.
- The Study Group conducted an **all-day tabletop "stress test" of the electric grid** (in a localized area) under an extreme disaster scenario to uncover potential gaps in resilience.
- **An all-day CEO Roundtable** was convened to examine the results of the "stress test" and consider practices and policies for industry and government to enhance resilience in the electricity and nuclear sectors.

We believe these extra dimensions helped to inform private sector executives in a way that will better prepare them to engage public sector leaders in addressing sector-specific resilience issues and defining private and public sector roles.

Framework for Resilience in Critical Infrastructures

In designing and carrying out the electricity sector case study, a framework for setting, testing, and improving resilience goals emerged—one that we believe can be used to develop resilience goals and improve resilience practices in the other critical infrastructure sectors.

Although there are many definitions of resilience, the Council used the definition developed in our 2009 study as the basis of this overall study. In its simplest form, infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. This definition was used to develop a common construct to describe and organize resilience practices in the electricity sector. This resilience construct, originally conceived by resilience expert Stephen Flynn, consists of four outcome-focused abilities: (1) Robustness—the ability to absorb shocks and continue operating; (2) Resourcefulness—the ability to skillfully manage a crisis as it unfolds; (3) Rapid Recovery—the ability to get services back as quickly as possible; and (4) Adaptability—the ability to incorporate lessons learned from past events to improve resilience. This construct allows universal concepts of resilience to be understood and shared across critical infrastructure sectors and between industry and government.

Using this construct as an organizing guide, we uncovered a rich and diverse array of practices used by electric and nuclear companies to manage a variety of risks within both regulated and competitive business environments. For the companies in these sectors, practicing resilience is already a core operating principle and an integral part of their commitment to customers, shareholders, and communities. Millions of dollars are invested in minimizing the likelihood and impact of outages.

The electricity and nuclear sectors make extensive use of emergency and continuity planning, risk modeling, disaster drills, tabletop exercises, operator training, safety features, redundant and backup systems, advanced technologies, innovative organizational structures, mutual assistance, supply chain management, and other methods to manage a variety of everyday and uncommon risks. These practices are woven into the business functions, operations, and culture of both sectors. Companies we spoke with use every opportunity to incorporate new lessons from past events and drills to improve their resilience. Overall, the sectors have a remarkable record of safety, reliability, and efficiency while managing operational risks.

The Council believes that infrastructure resilience is a shared responsibility of the private sector, government, communities, and individuals. The growing complexity and interconnectedness of our critical infrastructures, the uncertainty of the emerging risk landscape, and the practical limitations of private companies to address certain risks all underscore the need for collaboration between the public and private sectors to strengthen infrastructure resilience. But *shared responsibility* does not necessarily mean the *same responsibility* or *historical responsibility*. Our case studies of the electricity and nuclear sectors highlighted the distinct functions and unique capabilities of the private sector in designing, building, operating, and maintaining increasingly complex infrastructures. The government helps to strengthen and sustain these functions by sharing risk information, providing a reinforcing regulatory environment, creating needed incentives to spur investment, and providing key resources during extreme disasters when the capabilities of the private sector are exceeded. The case study also revealed how the changing risk landscape is causing the private sector to rethink the traditional boundaries of service providers, customers, communities, and government in ensuring the reliability and resilience of the electricity and nuclear sectors. The following findings and recommendations are predicated on the belief that the partnership approach can unite the special capabilities and expertise of the public and private sectors to minimize infrastructure risks and improve resilience.

Findings

Our findings focus primarily on the electricity sector, which was the main area of study. However, many of the observations and issues apply equally well to the nuclear sector and other Critical Infrastructure and Key Resources (CIKR) Sectors.

Resilience in the Electricity and Nuclear Sectors

The U.S. electricity and nuclear sectors are highly reliable and resilient. However, the scope and depth of the resilience practices used routinely by these sectors are not well understood or communicated. The North American power system is designed and operated to absorb shocks, avoid cascading failures, and recover rapidly. This is enabled by rigorous planning, construction, and operating requirements; an interconnected, high-voltage, bulk power system in which generation and transmission is dynamically managed in a highly structured way; and a strong culture of commitment to reliability and mutual assistance. Although we found hundreds of examples of how power utilities mitigate risks in day-to-day operations, many of the practices are so ingrained in the operations and culture of the utility industry that many within the industry do not label them as resilience, and many outside the industry are unaware of the extensive resources expended to minimize all-hazard risks.

Electricity and nuclear sector practices suggest an implied set of sector goals based on the framework for resilience. The large number and variety of utility practices, strategies, and actions suggest several underlying resilience goals that the electricity and nuclear sectors have already adopted. These include: (1) Withstand a shock from any hazard with no loss of critical functions; (2) Prevent a power disruption from cascading into interconnected systems; (3) Minimize the duration and magnitude of power outages through rapid recovery strategies; and (4) Mitigate future risks by incorporating lessons from past disruptions, simulations and exercises, and sound risk assessment processes.

The Emerging Risk Landscape

The risk landscape is changing in ways that may affect both the reliability and resilience of the electric power sector. Extreme weather events force many utilities to reassess their emergency practices, business continuity plans, and system design. Now, a new set of risks such as targeted physical and cyber attacks, geomagnetic disturbances, and pandemics is emerging. Many of these risks are beyond the purview of a single company or even the entire industry and will require collaborative foresight

exercises and shared responsibility and investment. Meanwhile, customer requirements and new regulations are changing the way electricity is produced and managed. These changes place new demands on the electric grid that may affect reliability, stability, and system integrity.

Increased cyber monitoring and control of the electric grid has reshaped risks in ways that are not fully understood. The increased use of cyber-based control systems to manage transmission and distribution has increased system functionality and reliability, but has also introduced new risks in the electric grid. Digital control systems that share common infrastructure or connect to business systems for improved efficiency offer new opportunities for system control and security but may also expose the electric grid to cyber intrusions. Federal agency responsibility and capability regarding cyber vulnerabilities, information sharing, emergencies, and mitigations are still unclear to many utilities.

Cross-sector risks faced by the electricity sector include fuel supply, telecommunications and IT, transportation, and water. As one of the "lifeline sectors," the power sector is expected to operate when other infrastructures are out of service, and it does this quite well. Yet the power sector, in turn, relies on fuel supplies to power generators; water for cooling; data networks to operate control systems that manage power throughout the electricity system; telecommunication systems to contact emergency personnel; and transportation networks to deliver fuel, equipment, and personnel. For each dependency, the sector has developed redundant and backup systems.

Challenges and Opportunities to Increasing Resilience

The limited availability of extra-high-voltage transformers in crisis situations presents a potential supply chain vulnerability. Although utilities are quite adept at managing their equipment inventories and supply chains, extra-high-voltage transformers in particular may present a weak link in the sector's resilience. These transformers are highly specialized equipment, have 18- to 24-month manufacturing lead times, and are difficult to transport. Their high cost limits the ability of utilities to maintain many spares, which are often co-located at substations, thereby increasing their vulnerability. Industry programs to share spares help to mitigate risks, but the application of this arrangement has been limited in practice.

The ability of utilities to achieve greater levels of resilience is constrained by market, regulatory, and technical factors. The electricity sector has long-lived capital assets that turn over slowly at a time when the risk landscape is changing rapidly. Investments in reliability and resilience are not always seen by regulators as benefiting customers, and this limits the ability of utilities to recover costs. Difficulty in obtaining access to new rights-of-way limits the ability of the industry to expand transmission lines to relieve congested corridors and build better interconnections that increase resilience. Further, electricity must be delivered instantaneously; there are few cost-effective options for bulk storage.

Government information sharing on risks to the electricity sector has improved, but more can be done. There is growing evidence that the sharing of threat and risk information by the government with the private sector has improved. However, power companies still believe they are not receiving timely, actionable information to effectively manage certain types of risks. Key barriers include the difficulty in translating classified threat information into non-classified, actionable information and the limited number of clearances within utilities needed to receive classified information.

Restoration planning, including black start capabilities, provides an effective measure of recovery but deserves more focused attention. Despite excellent reliability and efficient rapid recovery capabilities, the electricity industry recognizes the risk of blackouts. Restoration planning for large-scale outages includes the contingency for a "black start" in which generation must be brought back online and the

grid restored without connected power sources. Although the industry regularly conducts live tests and exercises for this low probability event, additional planning, through current authorities such as independent system operators, regional transmission operators, and the North American Electric Reliability Corporation (NERC), may be warranted under certain scenarios.

Boards of directors at power companies receive a high volume of risk information, but it remains difficult to communicate and quantify operational risks in a rapidly changing risk environment. Boards today are operating in one of the most challenging business environments ever encountered; the rapid speed of change and the complexity of these new emerging risks means that boards have little lead time to identify approaching opportunities or changes and provide proper oversight. Emerging operational risks are difficult to quantify and balance with a traditional risk profile, making the efficient communication of potential impacts a challenge. The availability, quality, timeliness, and format of risk information presented to the board will affect the board's ability to provide meaningful oversight. In addition, increasing Federal initiatives and regulations aimed at mitigating operational risks diminish oversight power of the board of directors and introduce another layer of compliance concerns.

Recommendations

1. **The White House should initiate an executive-level dialogue with electricity and nuclear sector CEOs on the respective roles and responsibilities of the private and public sectors in addressing high-impact infrastructure risks and potential threats, using an established private sector forum for high-level, trusted discussions between industry executives and government leaders.** It is critical to create opportunities for public-private partnership using excellent models, like the Critical Infrastructure Partnership Advisory Council (CIPAC), that already exist. While these partnerships typically bring much-needed functional expertise to the table, most of the participating individuals are not empowered to make decisions for other parts of their organization or have the ability to influence sector CEOs on priority issues. What is needed is an executive-level forum of private sector CEOs and their government counterparts to focus on high-level policy issues; create a framework for public-private collaboration with defined roles and responsibilities; and make recommendations that strengthen overall resilience, especially for high-impact, low-frequency risks.

2. **The nuclear and electricity industries should each develop an emergency response plan that outlines a coordinated industry-wide response and recovery framework for a major nationwide disaster.** Although electric and nuclear utilities have robust emergency response plans and exercise them regularly, there is no industry-wide plan to address a major national disaster. Although relationships between the companies and their States, regions, and communities are well established, the relationships, roles, and responsibilities at the national level are less clear. The Council recommends that coordination and development of such an emergency response plan be led by CEOs in each sector and aligned with the National Response Framework and National Incident Management Systems. The CEO Business Continuity Task Force of the Electric Edison Institute (EEI) could lead this effort within the electricity sector, in coordination with NERC, the American Public Power Association, and the National Rural Electric Cooperative Association. The Nuclear Energy Institute could lead this effort within the nuclear industry.

3. **DHS and other Federal agencies should improve information sharing with the private sector by providing focused, actionable, open-source information on infrastructure threats and vulnerabilities.** While some information can only be shared in a classified setting, many of the useful incidents and trends can be culled from open sources and distilled into actionable recommendations to the private sector. The NIAC heard several examples of executives who gained key insights from analysis of open-source information that was tailored to their sector. DHS and other Sector-Specific

Agencies should work with their private sector counterparts through the CIPAC structure to identify the types of information that would be most valuable to owners and operators and the best mechanism to deliver it to them. DHS and other government agencies should develop more effective ways to share classified content with the electricity and nuclear sectors, or translate it into useful non-classified information.

4. **All critical infrastructure sectors should consider adopting the industry self-governance model exemplified by the Institute of Nuclear Power Operations (INPO) and the North American Transmission Forum (NATF) to enable the private sector to collaborate on industry-wide resilience and security issues outside the regulatory compliance process.** The nuclear industry created INPO as a private organization to address critical safety and reliability issues in the aftermath of the Three Mile Island disaster. Its defining feature is a self-governing model that commits each company to achieve excellence in nuclear power plant operations. This is backed up by plant evaluations that are shared confidentially within the nuclear sector, outside the regulatory process. More recently, the NATF has adopted this model to address transmission reliability and resilience issues across the electricity sector. These organizations create an opportunity to provide regular evaluations of the resilience and security of sector assets and systems, establish performance objectives, train and educate sector employees, and create CEO accountability for any shortcomings in performance. The self-monitoring nature of such an organization would not be a substitute for existing regulation, but would provide an extra measure of responsibility and care for overall industry performance.

5. **Promote the use of the NIAC-developed framework for setting resilience goals in the CIKR sectors and for providing a common way to organize resilience strategies within Federal and State governments and CIKR sectors.** The goal-setting framework developed by the Council should be used to help critical infrastructure sectors discern their resilience goals. The process enables sectors to not only establish outcome-based goals but also uncover gaps in sector resilience and develop options to address them. The process establishes a baseline of current practices, develops high-level resilience goals, tests the sector's resilience in a high-impact scenario, and addresses gaps and seams through a public-private dialogue. The process is flexible enough to be used by all CIKR sectors despite their differences in assets, businesses, and risk profiles. DHS should consider using this resilience framework as a common way to organize resilience strategies and programs.

6. **DHS should support modeling and analysis studies of the cross-sector economic impacts of CIKR failures using tools such as input-output analysis.** Many of the CIKR sectors are highly interconnected, which can improve resilience but also create new opportunities for problems to cascade across sectors, regions, and economic systems. Understanding the impact of sector failures is becoming more important as infrastructures become increasingly interconnected. The NIAC report, *Critical Infrastructure Partnership Strategic Assessment,* recommended that the government increase resources to conduct cross-sector studies and analyses, guided by private sector knowledge of infrastructure operations. The NIAC reaffirms this recommendation and highlights the need to place special emphasis on supporting studies that apply established economic models and tools to examine how increased interconnection affects infrastructure resilience and economic impacts.

7. **Federal and State agencies should allow cost recovery for utility investments that increase infrastructure resilience.** Utility investments in reliability and resilience beyond those required by existing regulations must be justified as benefiting the customers who will ultimately have to pay for them. To encourage the private sector to invest in the resilience of transmission and distribution systems, government agencies should modify their processes for allowing rate adjustments. For transmission systems, the Federal Energy Regulatory Commission (FERC) should initiate a rulemaking that enables utilities to recover costs of infrastructure investments that improve

resilience. For distribution systems and some transmission systems, the National Association of Regulatory Utility Commissioners or another appropriate body should issue policy recommendations to State utility commissions encouraging cost recovery for investments that improve resilience as part of their ratemaking process.

8. **Electricity industry and government leaders should pursue options to mitigate supply chain vulnerabilities associated with extra-high-voltage transformers.** Nearly everyone we spoke with recognized the supply challenges posed by extra-high-voltage transformers, including long manufacturing lead times, foreign production, large cost, highly customized designs, and difficult transportation logistics. Because maintaining spare transformers at all locations is extremely costly, the sector, through EEI, created a program that helps utilities to share their inventory of spare transformers and mitigate sector risks. However, the Council believes that additional steps are needed to further reduce supply chain risks.

   The Council recommends that the EEI Spare Transformer Equipment Program (STEP) be expanded and that EEI collaborate with NERC to determine the requirements for spare transformers for electric systems of various sizes. Additional options, including standardization of transformer design, development of a recovery transformer, and incentives to encourage additional domestic manufacturing of extra-high-voltage transformers, should be addressed as a priority issue by electricity sector CEOs and government executives through the executive-level dialogue outlined in Recommendation 1.

9. **The Federal government should work with owners and operators to clarify agency roles and responsibilities for cyber security in the electricity sector, including those for cyber emergencies and highly sophisticated threats.** The Federal regulatory framework and roles for all stakeholders involved in securing the electric grid should be clear to avoid duplicative or conflicting actions in times of crisis. The electric utility industry is not in the law enforcement or intelligence gathering business, and the government has limited experience operating the electric grid. Thus, each should be consulted, and the flow of information should be regularly exercised, before a threat becomes a crisis. To avoid confusion, those at the highest levels of government and industry should be involved in coordinating responses and declaring the need for emergency action. The electricity industry is also facing new highly sophisticated cyber threats, possibly from nation-states, that may exceed the capability and responsibility of owners and operators. The Council recommends that the White House work with electricity sector CEOs to clarify public and private roles and responsibilities in managing these cyber risks that could compromise the integrity of the bulk power system.

1.0 Study Overview

In October 2009, the National Infrastructure Advisory Council (NIAC or Council) issued, *Critical Infrastructure Resilience*, a study that examined how critical infrastructures could become more resilient. The study helped establish resilience as a fundamental concept for sustaining and enhancing infrastructure capability. In February 2010, the Department of Homeland Security (DHS) published the *Quadrennial Homeland Security Report: A Strategic Framework for a Secure Homeland (QHSR)*, which established a new strategic framework for the DHS. Resilience is one of three core concepts within this framework to provide a comprehensive approach to homeland security:

- Security: Protect the United States and its people, vital interests, and way life
- Resilience: Foster individual, community, and system robustness, adaptability, and capacity for rapid recovery
- Customs and Exchange: Expedite and enforce lawful trade, travel, and immigration

Resilience helps to mitigate risk to communities, enhance recovery capabilities, and ensure continuity of essential services and functions. Accordingly, the QHSR established two core resilience objectives:

- *Broad-based resilience*: "Improve capabilities of families, communities, private-sector organizations, and all levels of government to sustain essential services and functions"
- *Infrastructure resilience*: "Enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions"

A Framework for Establishing Critical Infrastructure Resilience Goals is one of two 2010 NIAC studies that build on these QHSR resilience objectives. This study and its companion study*, The Optimization of Resources for Mitigating Infrastructure Disruptions,* extend the work done in the NIAC's 2009 *Critical Infrastructure Resilience* study by assessing the infrastructure/community interface and establishing a model for infrastructure resilience goals.

The NIAC recognizes that resilience is an important strategy for managing all-hazard risks in critical infrastructures. Our 2009 study, *Critical Infrastructure Resilience,* provided a common definition of resilience and observed that each sector applies resilience strategies and practices in different ways based on its sector structure, asset configuration, risk profile, and business conditions. The NIAC recommended that "*Government should establish a collaborative dialogue with CIKR owners and operators in each sector to develop a commonly agreed-upon set of outcome-focused goals for each sector."* Once established, these goals can provide the basis for guiding industry and government resources to improve infrastructure resilience and outlining policy initiatives that can address potential gaps. The study also noted that *"resilience policy cannot be applied equally to all sectors but rather understood and analyzed on a sector-by-sector basis, taking into consideration the complexity of existing regulatory and voluntary protection programs, the fundamental nature of the sector, and the cost and benefit of potential resilience programs."*

To pursue these recommendations, the Council decided, with the support of the Under Secretary for the National Protection and Programs Directorate given on behalf of the Secretary of DHS, to conduct a study to describe and clarify sector-specific resilience strategies and practices, and how they can serve as the basis for setting resilience goals for each critical sector.

Objective

This study examines how resilience is defined and practiced within selected sectors and provides a framework to enable all Critical Infrastructure and Key Resources (CIKR) Sectors to set sector-specific resilience goals and ultimately enable them to improve resilience. Three objectives were established for this study:

- Assess how the selected sectors define resilience and use resilient practices to mitigate risk;
- Determine if and how resilience goals are established within the sector that lead to an accepted and understood policy and process for setting goals in each sector; and,
- Recommend government policies that will promote development of sector-specific resilience goals.

In addition, the study provides a process by which sectors can examine their resilience under extreme conditions, uncover potential gaps and seams, and identify policies and practices to address any shortcomings or barriers.

Scope

The Council believes that it is the purview of individual companies and sector-wide organizations and institutions to set resilience goals; as such, we did not set goals in either case study. Instead, we sought to understand how the NIAC definition of resilience manifests within specific sectors to help outline a process by which sector goals can be developed and tested. This process can then be used by each sector, as appropriate, to voluntarily develop goals that match their unique circumstances. By doing so, the government policies and programs intended to improve infrastructure resilience can be tailored to the special needs of each sector to achieve maximum results.

The electricity sector is the primary focus of the two case studies because the nuclear sector had already undergone a voluntary process to improve sector protection and resilience. Between 2005 and 2007, all 104 of the Nation's nuclear power reactors participated in the Comprehensive Review process with DHS to identify enhancements to facility protection and resilience beyond the stringent security standards already in place through regulatory agencies. The Council drew upon the Comprehensive Review approach to develop the electricity case study and documented the nuclear experience through discussions with the Nuclear Energy Institute (NEI).

Overall Study Approach: Developing a Framework for Establishing Critical Infrastructure Resilience Goals

A case study approach was used to achieve the overall study objectives. This allowed us to develop a preliminary framework and process for building a resilience goal structure that can apply to all CIKR sectors, yet still address the unique characteristics and requirements of each individual sector. This framework is described in detail in Section 3. This document contains the first case studies, using the electricity and nuclear sectors, and tests this preliminary framework, which can be applied and refined in subsequent case studies. This will help validate the robustness of the framework and improve upon any shortcomings.

Each sector case study includes four basic phases:

Phase 1 – Define sector resilience, practices, and strategies.

Phase 2 – Develop/test a framework for setting sector resilience goals.

Phase 3 – Assess the robustness of a sector's resilience.

Phase 4 – Identify government policies and industry initiatives to promote development and achievement of sector resilience goals.

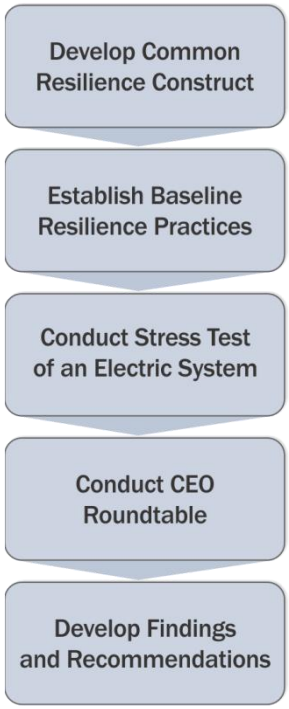
With the completion of this report, two sectors have now successfully used this approach to generate gaps and seams in responding to high-stress scenarios, and begin identifying improvements based upon those gaps and seams that would strengthen sector resilience in a variety of less stressful scenarios as well. The completed case studies demonstrate the ability of this process to generate resiliency improvements and should be considered as the template approach for other sectors.

Approach to the Electricity and Nuclear Case Studies

Although the electricity and nuclear sectors share many common characteristics, they also differ in many ways when it comes to security and infrastructure resilience. The protection of nuclear facilities, for example, is a top national priority and is highly regulated by the Nuclear Regulatory Commission (NRC) due to the need to safeguard nuclear materials and protect the public. The Comprehensive Reviews completed by the nuclear sector tested the robustness of their security practices and overall resilience. These reviews are well documented but contain certain classified information. Therefore, we focused the case studies on assessing resilience within the electricity sector using this model. The non-classified findings of the nuclear sector Comprehensive Reviews were documented through meetings between NIAC support staff and representatives of the Nuclear Energy Institute and are summarized in this report.

The electricity sector case study centered on the generation and transmission capabilities of the electricity sector. Although the resilience of distribution assets is important, electric grid performance is driven by the ability of the bulk electric power system to deliver reliable power to distribution systems throughout the United States and Canada. Accordingly, the 18 Study Group members (listed in the Acknowledgements at the front of this document) included CEOs of electric utilities, executives with transmission responsibilities, experts in physical and cyber security of the electricity sector, and leaders in resilience policy and corporate risk management. The key steps used to develop the electricity sector case study are shown in Exhibit 1.1.

Exhibit 1.1 Approach to the Electricity Sector Case Study



Using the definition of resilience developed in the 2009 NIAC study on resilience, the Study Group developed a common construct to describe and organize resilience practices in the electricity sector. This resilience construct, originally conceived by resilience expert Stephen Flynn, consists of four outcome-focused abilities: (1) Robustness—the ability to absorb shocks and continue operating; (2) Resourcefulness—the ability to skillfully manage a crisis as it unfolds; (3) Rapid Recovery—the ability to get services back as quickly as possible; and (4) Adaptability—the ability to incorporate lessons learned from past events to improve resilience. This construct allows universal concepts of resilience to be understood and shared across critical infrastructure sectors and between industry and government.

To establish a baseline of resilience practices within the electricity sector, the Study Group:

- Conducted 18 interviews with utility executives and managers of T&D operations

- Conducted 20 weekly Study Group discussions on key resilience topics
- Reviewed more than 100 studies and documents related to resilience and electric grid operations

The Study Group then designed and conducted a full-day tabletop exercise of the Baltimore Gas and Electric utility system that was designed to "stress" the system to the breaking point in order to expose gaps and find ways in which resilience could be strengthened. Additional exercises conducted previously by the North American Electric Reliability Corporation (NERC), DHS, and the U.S. Department of Energy (DOE) were also studied and analyzed.

The Study Group next convened a CEO Roundtable that reviewed information developed in the electricity sector study and the results of the stress exercise to identify resilience enhancements in the context of business models and possible roles for the public and private sectors.

The information gathered—through interviews, weekly discussions, literature review, analysis of the nuclear sector Comprehensive Reviews, the tabletop stress exercise, and the CEO Roundtable—was used to develop the findings and recommendations contained in this report.

2.0 Defining Resilience

The study began with a charge to assess how sectors define resilience, and then determine if and how resilience goals are established within the sectors.

The NIAC Definition of Resilience

Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.

We learned through our previous work that critical infrastructure sectors define resilience in different ways and employ different principles and practices that are aligned with a particular definition. The overarching definition of infrastructure resilience contained in the Council's 2009 report, *Critical Infrastructure Resilience,* has provided a good starting point for developing a common language about resilience. However, each sector uses different terminology that is rooted in their history, culture, operations, and business environment. Any effort aimed at improving resilience within critical infrastructure sectors must first recognize the different terminology and approaches sectors use to manage risks.

The predominant risk management concept within the electricity sector is *reliability*. The electric grid is a highly interconnected system of generating plants, high-voltage transmission lines, substations, distribution systems, and other assets. Because electricity cannot be stored, it must be generated as it is needed and supply must be kept in balance with demand. Furthermore, electricity follows the "path of least resistance" and generally cannot be routed in a specific direction. This means generation and transmission operations in North America must be monitored and controlled in real time, 24 hours a day, to ensure a consistent and ample flow of electricity. This requires the cooperation and coordination of hundreds of electricity industry participants.[1] In short, reliability is the ability to meet the electricity needs of end-use customers, even when events reduce the amount of available electricity.

The primary concern of the electricity sector is the reliability of the *bulk power system*—the essential generation and transmission backbone of the electric grid. Although individual utilities are very concerned about maintaining power to their customers through their distribution systems, the sector as a whole relies on and is committed to maintaining the integrity of the bulk power system.

NERC defines the reliability of the interconnected bulk power system in terms of two basic and functional aspects:

- **Adequacy—**The ability of the bulk power system to supply the aggregate electrical demand and energy requirements of the customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.
- **Security—**The ability of the bulk power system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system elements from credible contingencies.[2]

Risk management within the electricity sector is concerned with (1) the likelihood that an event will reduce the reliability of the bulk power system and its interconnections, and (2) the consequences if it does.

All of the electricity sector executives we spoke with mentioned reliability as the guiding objective of the sector and offered similar explanations of core concepts and principles. They also shared a common

[1] NERC, "About NERC: Understanding the Grid."
[2] NERC, *Reliability Concepts*.

understanding of the NERC standards for planning and operating the electric grid that are used to achieve high levels of reliability. However, when asked to define resilience in the electricity sector, their perspectives varied. While reliability is generally viewed as "keeping the lights on," resilience was viewed by some as the ability to recover rapidly when the lights go out. Others we spoke with viewed resilience as a much larger concept that encompasses all aspects of reliability. Some talked about resilience as the ability to ride through events and bring back facilities after an event. Resilience was also described as an element of the overall electric system design: the capacity of a large interconnected grid to absorb shocks. One executive contrasted resilience (the ability to take a hit and recover) with redundancy (having at least one backup available if a component fails). Most executives we talked with indicated that while reliability is relatively easy to define and measure, resilience is more difficult.

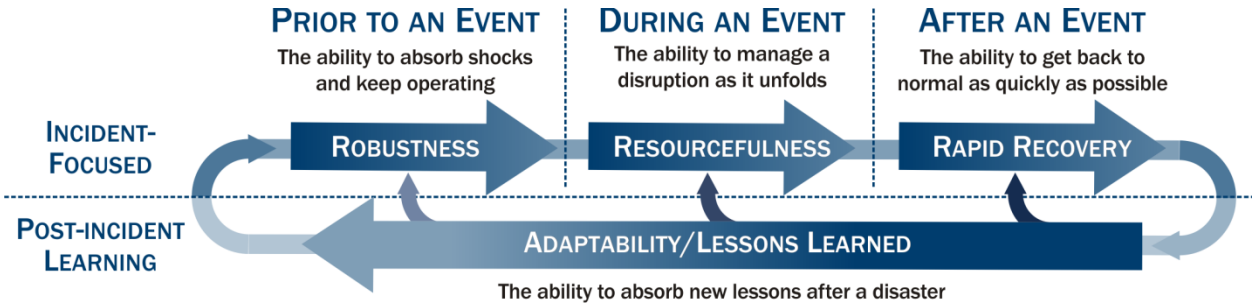
With no universal definition of resilience, the electricity sector has not developed sector-wide outcome-based resilience goals. Instead, owners and operators see reliability as the overriding goal for the sector and have established a variety of standards, guidelines, and regulations to achieve it. Yet this does not mean that electric utilities do not diligently pursue resilience practices.

Specific definitions of resilience are less important than fundamental concepts of resilience. Through our interviews and research we uncovered an impressive array of risk management practices that are commonly used throughout the sector. To organize and describe these practices, we relied on a construct for resilience originally conceived by resilience expert Stephen Flynn. The construct is based on four features:

- **Robustness**—The ability to keep operating or to stay standing in the face of disaster. In some cases, it translates into designing structures or systems to be strong enough to take a foreseeable punch. In others, robustness requires devising substitute or redundant systems that can be brought to bear should something important break or stop working. Robustness also entails investing in and maintaining elements of critical infrastructure so that they can withstand low-probability but high-consequence events.
- **Resourcefulness**—The ability to skillfully manage a disaster as it unfolds. It includes identifying options, prioritizing what should be done both to control damage and to begin mitigating it, and communicating decisions to the people who will implement them. Resourcefulness depends primarily on people, not technology.
- **Rapid recovery**—The capacity to get things back to normal as quickly as possible after a disaster. Carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right places are crucial.
- **Adaptability**—The means to absorb new lessons that can be drawn from a catastrophe. It involves revising plans, modifying procedures, and introducing new tools and technologies needed to improve robustness, resourcefulness, and recovery capabilities before the next crisis.

The Study Group organized these features into a sequence of events shown in Exhibit 2.1. Robustness includes the measures that are put in place prior to an event; resourcefulness includes the measures taken as a crisis unfolds; rapid recovery includes the measures taken immediately after an event to bring things back to normal; and adaptability includes the post-incident measures and lessons learned that are absorbed throughout the system.

Exhibit 2.1 The Sequence of the NIAC Resilience Construct



Another dimension of resilience is time. The electricity system consists of massive amounts of expensive, long-lived capital assets that have relatively slow turnover. In the near term, system infrastructure and assets are fixed and utilities rely on practices that involve people, plans, processes, and procedures to improve resilience. Most practices can often be accomplished with short lead times and are typically less expensive than capital improvements. In the long term, however, utilities can introduce new technology and alter the design of the electric system to increase resilience. These measures are typically more expensive and require longer lead times, but may offer more enduring resilience because the security is "built into" the infrastructure. Based on these distinctions, the Study Group divided each of the four resilience categories into those practices involving people and processes, and those involving infrastructure and assets. We refer to this entire organization as the **NIAC resilience construct.**

Finally, the Study Group recognized that not all threats are addressed in the same way. Unintentional acts, such as storms, floods, earthquakes, and equipment failure, are a part of everyday operations that utilities can prepare for through plans, drills, and direct experience. Intentional acts, such as theft and targeted physical attacks, are harder to plan for and require different practices and strategies. Cyber acts, which can be accidental or malicious, represent a newer form of disruption that requires a special set of resilience practices.

Through interviews and research, the Study Group identified more than 100 examples of electricity sector resilience practices. These practices were organized into the NIAC resilience construct and presented in a full matrix in Appendix B. That matrix is not intended to present an exhaustive list of practices, but rather a representative sample. A summary of representative practices is shown in Exhibit 2.2.

Exhibit 2.2 Summary of Resilience Practices from NIAC Resilience Matrix of the Electricity Sector

	Robustness	Resourcefulness	Rapid Recovery	Adaptability
People and Processes	• Announced and unannounced emergency drills for control centers • Extensive continuity of operations plans	• Highly trained and drilled transmission operators • RTOs prevent cascading failures	• Mutual aid agreements • Priority recovery of electricity services for customers (e.g., hospitals, fire, police)	• Revising emergency response plan after Hurricane Katrina • Revised industry standards after 2003 blackout
Infrastructure and Assets	• Interconnected grid provides enormous absorptive capacity • Double-redundant transmission sections to handle N-2 failures	• "State estimators" enable real-time monitoring of transmission • Automated system transfer for N-1 failure	• Shared inventory of spare extra-high-voltage transformers • Spare transmission towers for rapid reconstruction (24 hr)	• Substations placed on stilts after major floods • Derated underground power line based on reported failure in another utility

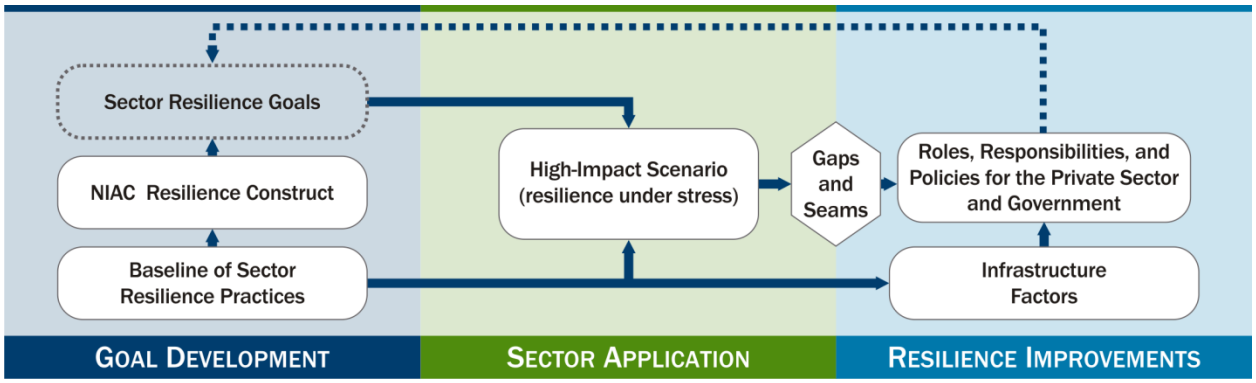
3.0 Framework for Establishing Resilience Goals

Developing a commonly agreed-upon set of outcome-focused goals for each sector is challenging. Each subsector, industry segment, owner, and operator has particular business, security, and operational needs. Sector goals that are too specific may not be appropriate for all businesses, while high-level sector goals may be too broad to be meaningful in guiding the development of resilience strategies for individual business. Many sectors also do not have a single organization or body that has the authority or convening power to develop appropriate goals for the entire sector.

Despite these challenges, the Study Group was able to develop a common framework and process for discerning sector resilience goals based on its study of the electricity sector. This framework can serve as a model for adoption by other CIKR sectors.

The framework consists of three interconnected elements shown in Exhibit 3.1: goal development, sector application, and resilience improvements.

Exhibit 3.1 Framework for Establishing Resilience Goals



Goal Development

The first step is to establish a **baseline of current resilience practices**. In our case study of the electricity sector, we documented hundreds of specific planning, security, business, and operational practices that contribute to the resilience of individual companies and the sector as a whole. We examined practices designed to address a variety of potential physical and cyber risks caused by natural weather events, accidents, aging equipment, malicious acts, and supply chain disruptions. We examined a full range of practices from company-specific procedures and practices to sector-wide planning and the architecture of infrastructure assets. Collectively, these practices define the current situation of resilience within the sector.

The second step is to describe and organize these practices according to the type of resilience capability it provides using the **NIAC resilience construct** described in Section 2. The four main organizing principles include robustness (absorbability), resourcefulness (real-time crisis management), rapid recovery, and adaptability (uptake of lessons learned). In our case study, we also distinguished between those practices related to people and processes and those related to the structure of infrastructure and assets for each of the four categories. Additional distinctions were made for practices related to unintentional acts, intentional acts, and cyber events.

The third step is to discern a set of **prospective sector resilience goals** that are implied by these practices. The purpose of this effort is not to establish final sector resilience goals but rather to propose

potential resilience goals that align with the current practices of the sector. For the electricity sector, the baseline of resilience practices organized within the NIAC resilience framework produced a set of high-level goals that aligned well with the way the sector plans and manages reliability for the electric grid. They are:

1) Withstand a shock from any hazard with no loss of critical functions.
2) Prevent a power disruption from cascading into interconnected systems.
3) Minimize the duration and magnitude of power outages through rapid recovery strategies.
4) Mitigate future risks by incorporating lessons from past disruptions, simulations and exercises, and sound risk assessment processes.

Sector Application

To test the robustness of the prospective sector resilience goals, the fourth step is to assess the resilience of the sector using a **high-impact scenario**, one that introduces risks that are well outside the typical or historical risks faced by the sector, and well beyond the scenarios it has adequately prepared for in meeting business and regulatory requirements. Used effectively in the nuclear sector's Comprehensive Review process and replicated for the electricity sector case study, this assessment can be accomplished using several different methods including tabletop exercises, modeling and simulations, engineering studies, and other means. For the electricity sector case study, we conducted a dedicated full-day tabletop exercise of the Baltimore Gas and Electric utility system that involved malicious catastrophic attacks on multiple substations. The scenario was specifically designed to cripple the utility at strategic locations. We augmented this tabletop with the results of other electricity sector tabletop exercises and studies including three scenarios from the NERC *High-Impact, Low-Frequency Event Risk* study and two scenarios from Secure Grid '09.

The assessment is designed to reveal **gaps and seams** in the resilience practices of the sector. The gaps and seams highlight circumstances in which the sector is unable to achieve the prospective sector resilience goals. By specifically stressing the sector beyond currently anticipated risks, we were able to gain insight into the types of resilience improvements that would enable the sector to better respond to not only a high-impact scenario, but also a range of less significant scenarios. In the various high-impact scenarios used in the electricity sector case study, a number of gaps were exposed, including mechanisms for coordinated public-private action, substation vulnerabilities, a lack of utility experience in responding to targeted physical attacks, and uncertainty of government roles during a major cyber attack.

Resilience Improvements

The true value of developing prospective sector resilience goals, testing them in extreme scenarios, and exposing gaps is that the process reveals opportunities to improve resilience. Invariably, the gaps and seams raise fundamental issues about the respective **roles and responsibilities of the private sector and government** in paying for and implementing security solutions. In our interviews, nearly every executive was able to identify opportunities to improve sector resilience but indicated that most were either far too costly or were needed more for national security objectives rather than business objectives. A high-level dialogue among industry executives or between industry and government is considered one of the best approaches for developing solutions and defining roles. In the electricity sector case study, we convened a CEO Roundtable to assess the gaps and seams exposed by the high-impact scenarios. The CEOs developed several solutions to address specific gaps and seams that have been integrated into our recommendations.

Exhibit 3.2 Infrastructure Factors Affecting Sector Resilience

1. **Infrastructure Design and Asset Characteristics**
    a. Interconnectedness: Are products and services mostly facility-based or systems-based? How reliant are individual providers on the operational integrity of the entire sector? How interconnected are sector assets?
    b. Asset Profile: Are the majority of sector assets tied up in long-lived capital assets? Does the sector have rapid equipment turnover that can absorb new technologies quickly?
    c. Product/Service Profile: Can the product be inventoried or is it delivered in real time?
    d. Design Limitations: Are there technical, social, environmental, or policy barriers that limit the ability to design more resilience into the infrastructure?
    e. Cyber Dependence: Are the operations of the infrastructure controlled by cyber assets? If cyber assets go down, can the infrastructure still provide products and services?
2. **Supply Chain Vulnerabilities**
    a. Availability of Critical Components: Are key components readily available? Are lead times and cost of critical spares acceptable?
    b. Domestic Sources: Are domestic manufacturing capabilities adequate?
3. **Sector Interdependencies**
    a. Dependencies: Can the sector function long without key inputs from other sectors? Are executives fully aware of inherent risks from sectors they depend on? If the sector is disrupted, how will it affect other critical infrastructure sectors?
    b. Co-Location: Are sector assets vulnerable due to co-location with other infrastructures?
4. **Sector Risk Profile**
    a. High-Profile Target: Is the sector a high-profile target for physical or cyber attacks?
    b. Strategic Assets: Does the sector contain assets that are critical for national security?
5. **Markets and Regulatory Structure**
    a. Regulatory Constraints: Do regulations create barriers to increased resilience?
    b. Market Structure: How do company size, industry concentration, and profitability affect the ability of the sector to finance investments to enhance resilience?
6. **Public-Private Roles and Responsibilities**
    a. High-Impact, Low-Frequency Risks: Are government and industry roles and responsibilities clearly understood for high-impact, low-frequency risks?
    b. Disaster Coordination: Are the responsibilities and expectations of the sector during a disaster clearly understood by the government and the public?
7. **Standards**
    a. Standard Bodies: Does the sector have an existing, highly regarded organization or body to create standards for the sector using a stakeholder process?
8. **Information Sharing**
    a. Threat Information: Does the sector have adequate access to timely, actionable threat information?
    b. Clearances: Do companies have a cleared executive who can receive classified information and commit company resources?
9. **Workforce Issues**
    a. Capabilities: Does the sector have a workforce with adequate technical operating experience? Is an aging workforce an issue?

One important input to this process is an analysis of **infrastructure factors** that reflect the conditions and circumstances that affect the ability of the sector to resource and implement solutions. For example, the ability of the nuclear sector—with 104 total plants operated by 32 companies—to implement security solutions is much different from that of the commercial facilities sector, which has thousands of owners and operators of facilities as diverse as office buildings, casinos, malls, and sports stadiums. Several key infrastructure factors were identified and discussed during interviews and weekly conferences. A sample set of infrastructure factors is provided in Exhibit 3.2, which can serve as an initial template for other critical infrastructure sectors. The final step in the framework is the development or modification of **sector resilience goals** that are informed by the public-private dialogue. Prospective goals can be modified to reflect specific risks and circumstances. In this way, both government and industry can clarify public and private responsibilities to address infrastructure risks for which there is little precedent and improve the overall resilience of national infrastructures.

4.0 Resilience Practices in the Electricity and Nuclear Sectors

The findings and recommendations of this report are drawn from two case studies: (1) the electricity sector—developed out of extensive interviews, a tabletop stress exercise, a CEO Roundtable, and a literature review; and (2) the nuclear sector—based on an examination of the Comprehensive Review process through discussions with the Nuclear Energy Institute. They revealed both similarities and differences that affect each sector's resilience practices. Both are part of the energy sector and both are highly interdependent: about a tenth of North America's electricity is generated by nuclear power plants, while nuclear reactors depend on a reliable source of offsite power for their safe operation and shutdown in the event of reactor problems. Both sectors are also highly dependent on advanced data communications and control systems to continuously monitor their operations in real time, and both are among the most regulated sectors of the economy. The major electric utilities in the United States with corporate units for nuclear power plant operation also have transmission and distribution units for the construction and operation of facilities for energy delivery. Both sectors are deemed critical to the nation's health, safety, and economic well-being.

There are significant differences between the sectors as well. Risk management in the nuclear sector centers around the physical protection and safety of 65 nuclear power plant sites, which contain radioactive nuclear fuel; risk management in the electricity sector is concerned with the uninterrupted operation of the bulk power system—a vast interconnected network of generating plants, transmission lines, and distribution facilities coordinated on a second-by-second level by hundreds of transmission operators and computerized systems spread throughout the nation. While there are very few companies licensed to operate nuclear power plants, there are hundreds of companies that provide for the reliable operation of transmission and distribution systems that deliver electricity to North American customers. Nuclear power plants have well-defined, secure perimeters, whereas electricity transmission and distribution lines are spread geographically across the entire country. Many nuclear sector executives have security clearances needed to receive classified security and threat information; the electricity sector is more diverse and only a very small percentage of its executives or other critical personnel are cleared to receive classified information from the Federal government.

Government and public concerns about the radiological risks, coupled with the small number of licensed operators within the nuclear sector, have resulted in a highly organized and coordinated approach to resilience enhancement beyond the security standards already in place through the Nuclear Regulatory Commission. The electricity sector, because of its decades-long focus on continuous and uninterrupted service, has tended to incorporate resilience enhancements beyond those specified by the North American Electric Reliability Corporation on an individual company basis—yet relies on the sharing of expertise and lessons learned to identify applicable resilience improvements across regions or the nation. As the following descriptions of resilience practices in the electricity and nuclear sectors show, the NIAC found a growing convergence between the two sectors in their approaches to resilience as the electricity sector begins to address risks far beyond those normally considered or encountered in the past.

4.1 Resilience in the Electricity Sector

More than 3,000 traditional electric utilities and seven regional transmission operators control a vast, tightly integrated system of generating plants, transmission lines, distribution facilities, and communication networks that operate and communicate simultaneously and in real time to provide electricity to residential, commercial, and industrial consumers. Commonly called the world's largest and most complicated machine, the North American electric grid, which covers the United States, Canada, and a small portion of Baja California Mexico, operates at 99.9 percent reliability, a feat that requires advanced monitoring and control technology and trained operators working in concert 24/7/365. System interconnection and close cooperation among utilities, power producers, and transmission operators enable the grid to withstand equipment failures and disruptive events while keeping the lights on.

Managing risk is an essential part of operating the electric grid. Maintaining the *reliability* of the electric system is the overriding objective for the sector and is the core of its risk management strategy. The sector views risk as the likelihood that an operating event will reduce the reliability of the electric grid to the point that the consequences are unacceptable. Because it is not possible or practical to prevent all disruptive events, the sector plans and operates the electric system so that when events occur, their effects are manageable and the consequences are acceptable.

The electricity sector understands that customers expect uninterrupted electricity service, and utilities do everything possible to meet this expectation. When disruptions occur, sector priorities are to 1) maintain real-time integrity of the bulk power system (to avoid a cascading blackout), and 2) protect the generation and transmission equipment from catastrophic damage (which could jeopardize reliability for weeks or months).

Reliability is built into every level of the bulk power system, the generation and transmission backbone of the grid. Redundancy is built into the system by interconnecting multiple transmission lines that enable electricity to flow from where it is produced to where it is used, even when some lines are forced out of service. Circuit breakers and other technologies are used to isolate faults (short circuits) on parts of the system when they occur to maintain the overall integrity of the interconnected grid. Numerous transmission operators, who are trained and certified according to rigorous NERC standards, are on duty 24/7/365 in every grid control center. State estimator systems give transmission operators a real-time picture of power conditions, enabling them to identify and isolate problems and correct for them before they cascade. One CEO told us that some state estimator and energy management systems have more than 700 contingencies to model effects if a given component fails or should be taken out of service. State estimators can be run continuously in the event of a contingency, and while the grid is highly automated, operators have the training, ability, and authority to bypass the automated response and manually reconfigure the system to shed or otherwise distribute customer load to ensure the grid's continued reliable operation, or minimize the impact.

Risk management, reliability, and recovery are so ingrained into the operation of the electric grid that the executives we interviewed don't often think of their practices as resilience. Electric utilities are very experienced in emergency response and recovery, and have evolved risk management models that help predict the impact of weather, unforeseen equipment failure, and natural disasters, enabling them to more effectively prepare. Utilities learn new lessons from every event and integrate improvements back into the grid in the form of training, improved practices, and new technologies that ensure better stability and response. This careful and purposeful evolution of the grid has enabled it to meet an electricity consumption rate that is more than five times what it was 50 years ago.

An evolving risk profile and new threats to grid resilience, however, are causing grid operators to prepare for risks outside of their traditional experience and responsibilities. Grid resilience is entering an area of joint responsibility where a coordinated industry and government approach is imperative.

This section examines the infrastructure and design of the grid, how it operates under regulation, how the sector talks about and practices resilience, and the factors facing the grid today that have CEOs calling for a dedicated, high-level partnership with their government counterparts.

Assets and Infrastructure Design

Because electricity cannot be easily stored, electricity must be generated and transmitted as it is used. As a result, the grid is managed in a highly structured way, using market mechanisms and coordinated transfers of electricity to continuously balance electricity generation and customer demand. Electricity generation, transmission, and distribution facilities are complemented by computerized systems at utility control centers that use a variety of digital sensors and field devices to monitor and control the grid over various communications networks. See Exhibit 4.1 for a brief overview of the electricity sector.

Overall, the electricity infrastructure is designed with reliability, efficiency, and cost-effectiveness foremost in mind. As a result, equipment tends to be physically large, capital-intensive, and have a long life; additional redundancy and backup equipment that would enable better reliability and more rapid recovery becomes both expensive and difficult to site. A targeted attack on extra-high-voltage transformers, for example, has been identified as a concern and a potential system vulnerability. Besides being very expensive, large, and hard to move, spare transformers have a long lead time in their production. Most are manufactured overseas, and must be custom designed to fit into the location-specific grid configuration.

Long recognizing this concern, electricity sector executives we interviewed said they are working within their utilities and through industry programs on several mitigating strategies. The electricity sector is taking the following actions:

- Reduce co-location of spare transformers with the units they intend to replace to avoid damage to spare units when operating units fail.
- Increase the number of spare transformers in the Edison Electric Institute (EEI) Spare Transformer Equipment Program (STEP), a coordinated industry program to build up the inventory and streamline the delivery process in the case of a disaster.
- Research and develop a recovery transformer to use temporarily until a new transformer can be ordered, built, shipped, and installed.
- Research the possibility of building standardized transformers to reduce the number of uniquely designed units.

Highly sophisticated control systems, too, are expensive and have a 10- to 20-year life span. With the rapid pace of change in technology, however, systems and equipment become outdated quickly and technology upgrades require add-on components, rather than substantial replacements. Given the need for these systems to be in continuous operation, all changes must be implemented without disruption. The electric grid has evolved over many decades, and is no longer the optimal design considering these new and emerging risks. If the system were to be redesigned today, there would be opportunities to build more security into equipment and systems, build critical components such as high-voltage transformers to more uniform standards, better integrate distributed and renewable energy, and easily integrate advanced digital controls for the smart grid.

Exhibit 4.1 Electricity Sector Profile

Elements of the Sector

Generation: More than 17,000 power generators convert primary energy sources including coal, nuclear, natural gas, oil, and renewable power—such as hydropower, biomass, wind, and solar—into electricity. Generators are capital-intensive and often located in remote areas.

Transmission: As electricity transport is most efficient at high voltage, transformers at generating stations step up low-voltage power from generation plants and use 211,000 miles of high-voltage transmission lines to move power over substantial distances to distribution systems, where transformers step down the voltage for customer use.

Distribution: Distribution substations lower the voltage of electricity and send it through a network of lines that deliver it to businesses and residences.

IT and Communications Networks: Computer control systems monitor and control generation, transformer operation, and electricity flow through the transmission and distribution systems, as well as supporting cooling, waste heat recovery, and emission control systems. Control networks allow operators to balance supply and demand in real time—paramount to reliability—and enable market exchange of electricity.

Ownership and Market Regulation

State-level Public Utilities Commissions (PUCs) or Public Service Commissions control retail rates to customers of **investor-owned electric utilities** that serve about 71% of ultimate electricity customers. As private businesses, these utilities are subject to State and Federal tax and are responsible for producing a profit for their stockholders. In many geographic areas, they are granted service monopolies, but required to charge reasonable rates that are comparable for similar classifications of customers, and must give customers access to services under similar conditions.

State- or municipal-owned and rural electric cooperative utilities are regulated either by States, local municipal officials, or elected boards, and typically either generate or distribute power. Both provide services at cost, and return a portion of their net income to their customers. Publicly owned utilities are non profit and are not subject to State and Federal income tax. The nine **Federal electric utilities** operate within several U.S. agencies and the power they produce is primarily sold wholesale to municipal and cooperative utilities. **Independent power producers** sell power at market-based rates subject to FERC authorization.

It is much harder to retrofit the electric system than to rebuild it from scratch, one industry CEO said, but the time and expense of rebuilding the grid makes this impossible. Thus, as the grid becomes larger and more advanced, it also has the potential to become more vulnerable to reliability problems due to increased system complexity, congested transmission corridors, the variability of renewable generation sources, and ever-changing customer demands.

To enable the grid to anticipate and adapt to future risks and demands, several executives said they have increased long-term planning out to 10–20 years. One executive said his utility's transmission engineers use a power systems simulation model for long-range engineering that uses a base case to look at how systems will be built 10 years out and identifies where new construction will be needed along the way to ensure reliability. While resilience improvements must be made incrementally because of the nature of electricity sector assets, those changes are being planned to deliver cohesive, flexible systems that can meet future demands.

Designed for Reliability

Because the bulk power system is highly interconnected and interdependent, the system must be designed to achieve certain standards of reliability in order to minimize the possibility of cascading failures, prevent equipment damage, and ensure continuity of service.

The electricity sector operates to a standard commonly referred to as "N minus one," or N-1, meaning that each individual part of the system is operated in such a way that the failure of any one component (one contingency) will not disrupt the reliability of the overall system. This allows system operators time to make system readjustments in preparation for any subsequent component failures. The concept of

contingency operation and planning is embedded into NERC standards for the planning, design, and operation of facilities, networks, equipment, and other components for the bulk power system. CEOs said in many critical parts of the system, utilities have gone even further, constructing double-redundant transmission sections or using other methods to withstand more severe contingencies where the risk of system failure is unacceptable. In planning future systems, more severe simulations are performed, testing the ability and resilience of the system to withstand multiple contingencies (N-2 or more) without losing its integrity or experiencing widespread cascading outages.

Because the transmission system carries large electricity loads and is part of the bulk power backbone, redundancy is built into the system by interconnecting multiple transmission lines to allow electricity to flow from where it is produced to where it is used even when some lines are forced out of service, enabling uninterrupted flow of electricity. The system receiving the load can become stressed, however, increasing the likelihood of an additional failure; multiple failures within a transmission segment can cause cascading failures and result in regional blackouts. The electricity sector has a fundamental reliability objective of preventing local events from cascading through the interconnected bulk power system and shutting down major portions of the grid—as occurred during the Northeast Blackout of 2003 (see Exhibit 4.2). Enhanced technology, increased coordination, improved sensors, and specially trained operators now work together to isolate problems on the grid.

While the electricity sector is designed around the concept that localized failure at the distribution level will occur, that failure is isolated and repaired quickly by experienced utility emergency response crews. During extreme emergencies, grid operators may need to intentionally disrupt service to customers to maintain the integrity of the bulk power system, prevent cascading failures, and enable the utility to restore power quickly once the system is fully restored. Most outages occur at the distribution level from equipment failures or natural damage. To bolster the transmission and distribution systems, utilities implement NERC and Institute of Electrical and Electronics Engineers (IEEE) standards devised to ensure that the various components of the system are capable of handling significant events, such as wind loading, lightning, flooding, icing, and other physical stress.

Market and Regulation

The electricity sector operates in a highly regulated environment. At the national level, NERC develops and enforces reliability standards for the bulk power (generation and transmission) system. The Federal Energy Regulatory Commission (FERC) oversees NERC activities and holds regulatory authority over wholesale transmission and interstate power exchanges. Customer rate regulation occurs at the State/local level.

In regulated retail markets, investor-owned utilities typically operate on a vertically integrated basis, providing generation, transmission, and delivery service at a bundled price to retail customers. For those States that have adopted retail competition (deregulation) within organized wholesale markets, many investor-owned utilities have sold their generation services and placed their transmission assets under the operational control of not-for-profit transmission operators, including independent system operators (ISOs) and regional transmission organizations (RTOs).

The seven existing RTOs/ISOs have broad operational control over most utilities' transmission assets and are obliged to provide non-discriminatory transmission access to electricity generators and customers. They also operate competitive wholesale markets for energy services and demand response, and have authority over transmission system planning.

Exhibit 4.2 Northeast Blackout of 2003

Event Summary

Electrical, computer, and human errors combined to cause the widespread Northeast Blackout on August 14, 2003. At 12:15 p.m., incorrect data input rendered Midwest Independent System Operator's state estimator computer system monitoring tool ineffective. An hour later, First Energy's Eastlake 5 generation unit was tripped, followed by a failure of the alarm and logging system in the First Energy control room, preventing the control room operators from being notified of the degrading electrical system and triggering continuous computer failures.

A series of transmission line outages in northeastern Ohio beginning at 3:05 p.m. caused heavy loadings on parallel circuits, leading to the trip and lock-out of the Sammis-Star line just one hour later. Once this system outage occurred in the Cleveland-Akron area, power that was flowing into that area over those lines shifted onto lines to the west and the east. The trip and lock-out of the Sammis-Star line from the rapid increase in loading triggered a cascade of line outages on the high-voltage system, causing electrical fluctuations and generator trips that rippled from the Cleveland-Akron area, northward into Michigan, and up into Canada. Because of these cascading line trips, the entire northeastern United States and eastern Ontario then became a large electrical island separated from the rest of the Eastern Interconnection. By 4:10 p.m., minutes after the Sammis-Star line tripped, the blackout had spread across much of the northeastern United States and Canada.

Impacts

By 4:13 p.m., more than 508 generating units at 265 power plants had been lost, which affected an estimated 50 million people and more than 70,000 megawatts (MW) of electrical load in parts of Ohio, Michigan, New York, Pennsylvania, New Jersey, Connecticut, Massachusetts, Vermont, and the Canadian provinces of Ontario and Québec. Although power was successfully restored to most customers within hours, some areas in the United States did not have power for two days and parts of Ontario experienced rotating blackouts for up to two weeks.

Lessons Learned

The U.S.-Canada Power System Outage Task Force provided a total of 46 recommendations intended to prevent or minimize the scope of future blackouts. These recommendations encompassed four key themes:

1. Government bodies in the U.S. and Canada, regulators, the North American electricity industry, and related organizations should commit themselves to making adherence to high reliability standards paramount in the planning, design, and operation of North America's vast bulk power systems. Market mechanisms should be used where possible, but in circumstances where conflicts between reliability and commercial objectives cannot be reconciled, they must be resolved in favor of high reliability.
2. Regulators and consumers should recognize that reliability is not free, and that maintaining it requires ongoing investments and operational expenditures by many parties. Regulated companies will not make such outlays without assurances from regulators that the costs will be recoverable through approved electricity rates, and unregulated companies will not make such outlays unless they believe their actions will be profitable.
3. Recommendations have no value unless they are implemented. Accordingly, the Task Force emphasizes strongly that North American governments and industry should commit themselves to working together to put into effect the suite of improvements that the Task Force recommended. Success in this area will require particular attention to the mechanisms proposed for performance monitoring, accountability of senior management, and enforcement of compliance with standards.
4. The bulk power systems are among the most critical elements of our economic and social infrastructure. Although the August 14 blackout was not caused by malicious acts, a number of security-related actions are needed to enhance reliability.

Source: U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada*.

Cost Recovery

Infrastructure upgrades to improve resilience are often costly and difficult to justify if they do not provide an immediate or noticeable benefit to customers, such as improved day-to-day service. Utilities must answer to both regulators and investors or elected/municipal officials when considering how to equitably share the cost of reliability improvements. Customers may only see the benefits of resilience

enhancements in the event of a crisis or disaster, which might not happen for years, if ever. Regulation is designed to protect customers from rate hikes they would be unwilling or unable to accept, and makes it impossible to simply pass through all necessary upgrade costs to customers without extensive public consultation.

Critical Interdependencies

Other Sectors

While the power sector is designed to operate when other infrastructures do not, the electricity sector depends on **fuel** and **transportation networks** (including trucking, rail, and pipelines), needed to gain access to facilities and to deliver fuel and equipment. It also depends heavily on **telecommunications and IT networks**, used to control the transmission and distribution of electricity, which will become increasingly critical as smarter digital technologies (including smart meters) are integrated to enhance the flexibility and capability of the grid. These networks are also critical to business system operations and essential communications during an emergency. **Water** is used to generate the steam that drives electric turbines in power plants and cool equipment, while **chemicals** are used to treat the water and steam, as well as manufacture primary sources of energy. The **manufacturing** sector provides millions of pieces of equipment used by the industry in its daily operations, from microchips to multi-ton, high-voltage transformers.

While conducting our case study, we learned of several electricity sector incidents that underscored important lessons about resilience and interdependency. One such lesson was about the limitation of redundant systems and ways events can cascade across sectors. In April 2010, BGE experienced an electrical fire in one of its cables, which led to the damage of the adjoining cable and caused a loss of both kV circuits, resulting in a power outage in the Towson, Maryland area (see Exhibit 4.3). Other utilities that shared the same right-of-way, including telecommunications and IT networks, were also damaged. BGE was able to restore power to customers fairly quickly. Nevertheless, the pumps at the Towson Reservoir Pumping Station needed to be re-primed, resulting in an extended water outage for residents and businesses in the Towson area. In this example, the co-location of utilities caused an event in the electricity sector to cascade to other sectors, and an electric cable and its redundant cable had a single point of failure.

Exhibit 4.3 Baltimore County Electrical Fire of 2010

Event Summary

On April 7, 2010, an early morning fire on an electrical pole took out two main power lines—a primary line and an adjacent backup line—that fed into the Towson Reservoir pumping station, disabling power to the station and beginning a water shortage that depleted water tanks in neighboring communities.

Impacts and Restoration

Towson University canceled classes, 18 schools were shut down in Baltimore County, downtown businesses and restaurants had to cope without water for much of the day, and county employees were placed on liberal leave. Baltimore Gas and Electric Company (BGE) had to repair both overhead and underground power lines as a result of the fire. Power was restored by 6:15 p.m. and by 7:30, crews were priming pumps to restore water service to more than 200,000 affected customers.

City officials noted that the power line arrangement was not uncommon and that the occurrence of a fire where the two lines converged was a "freak accident." Immediately following the incident, the city asked BGE to come up with a cost to separate the power lines.

Source: Kay and Green, "Thousands in Baltimore County try to cope without water," *Baltimore Sun;* Fujii, "Pumping Station Repaired, Water Pumped Into System," *Channel 13 WJZ*; Schuh, "Baltimore Co. Raises Questions After Water Outage," *Channel 13 WJZ.*

Although we did not fully investigate the economic significance of resilience in this case study, we learned about research and analysis being conducted in this field. Input-output models, interoperability input-output models, econometric time series models, computational general equilibrium models, and regional economic models can all help in understanding the impact of resilience investments within a sector.[3] One study, led by economist Adam Rose, simulated the economic impacts of a terrorist attack on the Los Angeles power system. Without resilience, the researchers estimated economic losses of $20.5 billion in two weeks. With several forms of resilience measures, the loss was reduced to $2.8 billion.[4] While the electricity sector recognizes the importance of economic interdependencies, the executives we interviewed indicated that they may not be fully aware of the risks they face from other critical infrastructure sectors or the economic impacts that could cascade across sectors. More work needs to be done in this area, a common theme raised in previous NIAC studies.[5]

The Interconnected Grid

In addition to interdependencies with other critical sectors, the electric grid is heavily dependent on the electrical interconnections within itself, on which utilities rely for the real-time exchange of electricity and response to regional events or disruptions. In North America, the bulk power system is made up of four interconnected grids: the Eastern, Western, Texas, and Quebec Interconnections. The Western Interconnection has some limited connection to Mexico and the Eastern and Western Interconnections are fully integrated with most of Canada. While these interconnections have limited power flows to each other, within each interconnection, transmission operators control flows between individual utilities. Virtually all U.S. utilities are interconnected with at least one other utility. Wholesale competitive markets allow utilities to reduce power costs, increase power supply options, and improve reliability.

Utilities rely heavily on their neighboring utilities, making them an important resource to help facilitate rapid response and recovery. Along with agreements governing the trade of electric power, executives said they have detailed mutual aid and cooperative agreements in place that enable utilities to quickly exchange spare equipment and repair personnel in an emergency. The importance of these interdependencies is not taken lightly; generation, transmission, and distribution organizations conduct large-scale emergency exercises at least annually to test coordination and procedures during an event. Major utilities often conduct cross-discipline, cross-sector drills at least once and as many as four times a year, executives said.

The Electricity Sector Risk Profile

Historical Risks

Electric grid operators have decades of experience in weather emergencies and natural disasters and have built on that experience to integrate effective response and recovery capabilities into primary grid operations. Experience makes threats from aging infrastructure, hurricanes, floods, icing, and other physical stresses quantifiable and more manageable. Utilities have become experts in risk management, evaluating risks, weighing the cost and benefits of reliability upgrades, and in many cases sharing the

[3] Greenberg, Lahr, and Mantell, "Understanding the Economic Costs and Benefits of Catastrophes and Their Aftermath."

[4] Rose, "Economic Resilience;" Rose et al, "Business Interruption Impacts of a Terrorist Attack on the Electric Power System of Los Angeles: Customer Resilience to a Total Blackout."

[5] See, for example, NIAC, *Framework for Dealing with Disasters and Related Cross-Sector Interdependencies*; NIAC, *Critical Infrastructure Partnership Strategic Assessment*; NIAC, *Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce Report and Recommendations*; NIAC, *Cross Sector Interdependencies and Risk Assessment Guidance*.

cost of infrastructure improvements with customers, to which the utility can provide a quantifiable benefit.

What was striking in the NIAC's CEO interviews and Study Group discussions was the extent to which the sector extensively analyzes major natural disasters and incorporates lessons learned across the industry. NERC publications and national reviews of major sector events[6] contribute to this self reflection, but operational improvements stemming from these events are primarily driven by company executives who see it as part of their core responsibilities to customers, shareholders, and other stakeholders. For more discussion on this, see the Adaptability section in this chapter.

Emerging Risks

An efficient, reliable electricity supply has become a foundation for efficient operations and growth in other critical sectors, including transportation, banking and finance, water, healthcare, and telecommunications. As a result, national security, public health, and safety are now more closely tied to electricity sector operation than ever, giving each outage and failure a broader impact. As the nation moves to modernize the electric grid and integrate thousands of digital components, new cyber and operational vulnerabilities are appearing, while the power grid has been thrust in the national spotlight as a potential target for well-resourced adversaries. The risk profile of the electricity sector is moving beyond the realm of operator experience and effective risk management. Traditional risk models were not designed to accommodate these new threats and the impacts are hard to quantify, making it difficult for utilities to prioritize and justify investment in certain resilience upgrades. To operate in tomorrow's economy with the same record of reliability, the electricity sector must work with its public sector counterparts to address emerging risks, including those discussed below.

Cyber Security and the Smart Grid

Advanced control and computer networks and components, including thousands of intelligent sensors, smart meters, and field devices, will enable the real-time control that promises to build on the efficiency of today's grid and deliver a fast, secure, reliable, and self-healing grid of the future. Where once these control systems were proprietary and isolated, they are increasingly interoperable and connected to business, wireless, and other networks to enable efficient and reliable operation and integrate smart grid technologies. But these advancements have introduced new vulnerabilities and created cyber security challenges—it is universally one of the biggest areas of concern within the electricity sector, the Study Group found, and previous NIAC studies and similar high-level reports concur.[7]

Several Study Group members voiced concern over the fact that manufacturing of control systems and software for key equipment found in control centers is often outsourced overseas, creating supply chain vulnerabilities and providing the opportunity for adversaries to insert back doors or malicious code. The recently discovered Stuxnet malware—specifically designed to infect Siemens industrial control systems used in the energy, nuclear, and other critical sectors—exemplifies a potential ability for adversaries to deploy targeted, malicious cyber attacks. Initially delivered via an infected USB flash drive, Stuxnet is designed to leverage a combination of vulnerabilities to gain access to its target and inject code to

[6] See, for example, Rigby,"We can't end outages, but we can respond to them better," *The Washington Post*; U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada*; U.S. Federal Energy Regulatory Commission, "Order Approving Stipulation and Consent Agreement: Florida Blackout."

[7] See, for example, NIAC, *Convergence of Physical and Cyber Technologies and Related Security Management Challenges*; CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*; White House*, Cyberspace Policy Review*.

change a process.[8] Electric utilities are partnering with national laboratories and system vendors to assess their systems for vulnerabilities and develop patches or mitigations, and many large utilities are actively involved in Federal R&D initiatives aimed at hardening the sector against cyber attack. Some executives told us they maintain underground bunkers and redundant or backup control centers to enable continued critical operations during a cyber failure. Internal drills on cyber events are now common, and many industry executives participate in national exercises such as the 2010 Cyber Shockwave and Cyber Storm III, simulated cyber attacks designed to preview how the U.S. government and its private sector partners would respond in real time to a large-scale cyber crisis. It is clear that effectively addressing these risks on a national scale will require a coordinated approach within the electricity sector and with the Federal government.

But several executives said that current public-private coordination efforts fall short. Though the Federal government has been working with industry on cyber issues since the 1990s, industry is still unsure of which government agencies and officials are in charge during a cyber emergency and what authority they have. Though national intelligence agencies monitor the cyber threat, inadequate channels for information sharing leave industry unable to effectively identify their vulnerabilities and evaluate the impact of an attack.

Cyber security deserves increased attention from both the NIAC and through Federal research and development, the Study Group concluded. CEOs identified it as a priority point of discussion in executive-level meetings between industry and government.

High-Impact, Low-Frequency Events

A June 2010 study by NERC identified three high-impact, low-frequency (HILF) event risks now faced by the bulk power system, aiming to make these events a high-priority focal point for risk managers and policymakers. Those identified include a coordinated cyber, physical, or blended attack against the North American bulk power system; a major pandemic causing the loss of staff critical to operating the electric power system; and geomagnetic disturbances caused by either solar weather or a high-altitude detonation of a large nuclear weapon or electromagnetic weapon, causing widespread interruption of system operation or equipment degradation.[9] The July 2009 Secure Grid '09 tabletop exercise hosted by National Defense University identified similar events as significant risk issues.[10]

Besides the potential for a far-reaching impact, HILF events raise particular concern because specific risks are not well understood, they are costly to mitigate, and the respective roles of industry and government in addressing these threats are unclear. While the sector has a century of experience with natural disasters under its belt, it has limited experience with primarily human disasters—terrorism, coordinated attack, cyber criminals, and pandemic illness—which could drastically affect large regions of the nation. There also is little or no experience for the type of industry and government coordination a HILF event would require. In the case of a malicious attack, for example, little coordination experience exists to ensure repair crews are protected and allowed access to crime scenes in order to quickly restore service. Grid operators also need better tools to measure the national impact on customers of extended outages.

[8] Nakashima, "Stuxnet malware is blueprint for computer attacks on U.S.," *The Washington Post*.
[9] NERC, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*. Also, Kappenman, "Electric Power Grid Vulnerability to Geomagnetic Storms;" Partnership for Critical Infrastructure Security, *Addressing the Pandemic Influenza Threat: Preliminary Cross-Sector Readiness Assessment*.
[10] Pugh, "Secure Grid 2009: A DHS-DOE-DOD Joint Exercise."

As part of the study process, the group participated in a "stress exercise," hosted by Baltimore Gas & Electric (see Exhibit 4.4), to assess a major utility's ability to respond to a significant event far beyond normal utility preparation—and it revealed several important lessons:

- Engineering quick fixes can work, but the system will be unstable and temporary equipment would have to be torn out to enable complete reconstruction.
- Industry, government, and customers would have to adjust to new realities of a severely damaged grid and change expectations of service restoration.
- High-voltage transformers are the critical vulnerability; by itself, the STEP program is not a long-term solution.
- The Federal government can facilitate recovery, but must be careful not to hinder industry operations.
- Remedial solutions—such as backup generators, solar panels, air conditioner shut down, and rolling outages—can take pressure off a damaged system, but there is no silver bullet for full recovery of service in a short period of time.
- Mutual aid agreements and contractors can help in the recovery, but their equipment might not be compatible with local specifications.
- To facilitate coordination in an actual emergency, Federal, State, and local government personnel should participate in similar private sector exercises on a regular basis.

Exhibit 4.4 Electricity Sector Case Study Stress Exercise—June 22, 2010

Hosted by BGE in Baltimore, Maryland, this scenario-based tabletop exercise was designed to severely stress the transmission system of a major U.S. electric utility company to determine what additional enhancements might improve sector resilience. Participants included leadership and senior engineers from several utilities, as well as representatives from regional transmission organizations. Also participating were company security and emergency response personnel.

The scenario included a coordinated terrorist attack against transmission facilities in several locations within the company's service area. Simultaneous attacks occurred elsewhere around the country. The scenario was presented in near real time, so that participants could experience the unfolding events and lack of clarity such a crisis generates. The engineers were asked to respond to the evolving crisis, restore services to customers, and return to a normal operating state as quickly as possible.

The full-day event resulted in many insights, including major challenges posed by such an extreme event, the carefully timed steps required in service restoration, and the significant supply chain issues involved in rebuilding key installations. Also noteworthy were the coordination efforts required between the public and private sectors in responding to and recovering from a terrorist attack on public utilities.

Insufficient Information Sharing Mechanisms

While not a threat on its own, the lack of timely, actionable, and contextual threat information prevents the electricity sector from taking appropriate action against known risks. The flow of intelligence information on risks, threats, and vulnerabilities from the Federal government to private sector executives is especially inconsistent. According to a July 2010 Government Accountability Office report, 98 percent of the private sector expects timely and actionable cyber threat information from the Federal government, but only 27 percent of the private sector believes it is being provided.[11]

[11] U.S. Government Accountability Office, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*.

The Aurora vulnerability, unique to generating equipment and discovered by a Department of Energy national laboratory in 2007, was a prime example for industry executives we interviewed. While classified briefings brought critical vulnerability and mitigation information to the nuclear sector, the lack of clearances in the electricity sector left CEOs with limited briefings that included little information on the problem, only information on how to fix it. Many in the Study Group expressed great frustration on the part of industry and concluded that an executive-level clearance in all major companies is critical to effective information sharing—an issue well documented in prior NIAC studies.[12]

Though one executive said Federal and intelligence agencies are diligent about communicating a specific threat to those who might be affected, communication of general threat and vulnerability information happens within State DHS networks, which are expected to communicate them to utilities but lack a trusted, widely used channel. Beyond clearances, however, targeted and contextualized open-source information can provide great value to a wider audience of industry managers and operators. In fact, one executive who attended a secret-level briefing given by DHS reported receiving the greatest value from the non-classified, open-source information he received there.

Fusion centers in the intelligence community have begun including business representatives to address information sharing issues. The Federal government also offers mechanisms and tools—such as the DHS Homeland Security Information Network – Critical Sectors (HSIN-CS) and the FBI's InfraGard—which greatly facilitate the exchange of information between critical infrastructure owners and operators and various government agencies. Regular open-source news reports targeted to each sector save executives time in sifting through information and provide them useful and actionable information without a clearance. Two examples of open-source news reports available to the electricity sector include the DHS Daily Open Source Infrastructure Report, prepared by the DHS Office of Infrastructure Protection, and the Current Situation Report, a weekly news analysis of cyber risks prepared by the DOE Office of Electricity Delivery and Energy Reliability that is provided to select industry members and researchers.

Within industry, companies have well-established mechanisms to communicate because of the interconnectivity of the grid and their mutual interdependencies. In recent years, the sector has also moved toward the adoption of an internal means to share information securely and confidentially on newly discovered vulnerabilities, best practices, lessons learned from incidents, and more. The North American Transmission Forum (NATF), which is modeled closely on the Institute of Nuclear Power Operations (INPO) within the nuclear sector, provides a confidential forum for its 16 member transmission system operators to candidly share event information, best practices, and constructive feedback (see Exhibit 4.5).

Resilience Practices in the Electricity Sector

Understanding Resilience in the Electricity Sector

The predominant risk management concept within the electricity sector is *reliability*, as discussed in more detail in Section 2. In short, reliability is the ability to meet the electricity needs of end-use customers, even when events reduce the amount of available electricity—in other words, "keeping the lights on." While executives we interviewed shared common concepts of reliability, their perspectives varied when asked to define resilience in the electricity sector. Some viewed it as the ability to recover rapidly when the lights go out; others viewed it as a much larger concept that encompasses all aspects of reliability. Some talked about resilience as the ability to ride through events and bring back facilities

[12] NIAC, *Public-Private Sector Intelligence Coordination: Final Report and Recommendations by the Council*.

after an event. Resilience was also described as an element of the overall electric system design: the capacity of a large interconnected grid to absorb shocks. Specific definitions of resilience, however, are less important than fundamental concepts of resilience, which in the NIAC resilience construct include robustness, resourcefulness, rapid recovery, and adaptability.

Exhibit 4.5 North American Transmission Forum

The August 2003 blackout demonstrated a clear need for better coordination within the industry on transmission issues. NERC, as the electric reliability organization certified by FERC, established the Transmission Owners and Operators Forum to achieve this coordination. In early 2010, this forum separated from NERC to become the North American Transmission Forum (NATF), a voluntary, industry-led and funded organization to promote the highest levels of reliability of North America's electric transmission system.

Structured around the belief that the industry is its own best consultant, NATF offers members confidential channels for sharing open and candid information, lessons learned, and best practices outside the regulatory environment. Modeled after the highly effective Institute of Nuclear Power Operations (INPO), NATF aims to raise the bar beyond compliance to operational excellence by cultivating the expertise of its collective membership and sharing it within the industry.

The forum operates four interdependent program areas: practices, information sharing, metrics, and peer reviews. With commitment from both senior executives and staff experts with a broad knowledge base, NATF aims to lead change in the industry by sharing event information and lessons, providing direct feedback and constructive opinions, and benchmarking best practices. An underlying premise of NATF is that more leadership, not more standards, is the key to improved reliability of electric transmission.

NATF garners participation from more than 650 experts across its 59 utility members, who collectively deliver 83% of the total peak electricity demand in the United States and Canada. Members include investor-owned, State-authorized, municipal, cooperative, U.S. Federal, and Canadian provincial utilities. Any organization that owns, operates, or controls at least 50 circuit miles of integrated (network) transmission facilities at 100 kV or above; operates a "24/7" transmission control center with NERC-certified transmission or reliability operators; or has an open access transmission tariff or equivalent on file with a regulatory authority, may join.

NATF Executive Director Don Benjamin says that the Forum is drawing upon the success and lessons learned from INPO, which has gone through a 30-year maturation process. For example, 100% confidentiality among the members enables candid discussions and assessments of industry practices. As NATF matures, it hopes to build upon a strong level of trust among members to add key functions of INPO, such as independent company performance assessments, which has become a feature of INPO's success. Mr. Benjamin characterizes NATF as "the killer app for reliability."

These concepts are reflected in the daily operational and business practices that pervade the industry. What follows is an overview of current strategies and practices in each of the resilience areas, gained through interviews with industry executives, Study Group discussions, and a literature review.

Robustness: Planning and Risk Management Practices

Risk management is embedded into the processes, planning, practices, and culture of the electricity sector. It is characterized by the ability to quantify the likelihood and impact of an attack, assess the cost of failure against the cost of mitigation, and prioritize mitigation options. Companies use a variety of assessment tools to examine and evaluate risks, considering factors such as geological area, condition of assets and equipment, interconnectivities and interdependencies, and known threats. One executive reported using an enterprise investment management tool that develops scores based on cost, need, risk, and customer impact—scores that help companies prioritize needs and infrastructure investments. Others said they engaged Risk Management Committees within the company to look ahead at risk based on the company's past experiences and those of others to identify both known and potential risks and mitigation strategies. For planning over time, utilities employ long-range planning models that forecast power requirements and potential vulnerabilities over 10 years and beyond.

Recurring threats such as aging equipment and natural disasters are manageable; experience makes them quantifiable, more predictable, and offers clear examples of the consumer benefits of mitigation investments. However, traditional risk management tools are proving inadequate for HILF event scenarios and malicious attacks, such as terrorism, cyber attack, or insider sabotage, where threats, targets, likelihood, and impacts are not well understood. Targeted malicious attacks, for example, require new risk management practices because they reduce the value of system redundancy.

To address a growing risk profile, risk management strategies are shifting, two executives said. Building up response and recovery capabilities is both less expensive and more flexible than hardening or redundancy, as it enables utilities to respond to a wide variety of failures. Prevention of and protection from a specific event can be costly and leaves utilities vulnerable to remaining risks. Executives we interviewed report an increasing focus on strong response and recovery as a risk management strategy.

A concerted industry effort is also under way to improve risk oversight from Boards of Directors, which typically oversee CEOs' risk management responsibilities. The type of risk information presented to boards is critical; boards have little time to examine the 20–30 enterprise risks they are often presented with, so operators and managers are developing various tools such as heat maps to aid members in prioritizing these risks. Boards also grapple with accountability for cross-sector or cross-departmental risks, as responsibility is not singular nor clear cut.

Resourcefulness: Training, Exercises, and Drills

The electricity sector extensively uses training, exercises, and drills not only to improve and refine existing crisis response plans, but also identify assets and equipment that could benefit from reliability upgrades. Individual companies use similar approaches to training, exercises, and drills, although each company tailors its approach to its unique operating circumstances, including geographic location, greatest risks, company size and service area, and available resources, such as access to national laboratories.

Executives we interviewed said they employ a variety of the following training, exercises, and drills:

- Business continuity drills, often utilizing a "hot site" to duplicate real-world conditions
- Stress exercises to deliberately "break" the system in order to find gaps in resilience
- Tabletop exercises with compounding effects reaching deep within the company and into bordering service areas
- Announced and unannounced drills
- Joint drills with city and county agencies
- Annual coordination meetings with responders to talk about recent events and identify lessons learned and best practices
- Tabletop exercises for black start situations to recover from a complete shutdown of the system
- Use of vulnerability response teams to test and exercise emergency response plans across the company
- Hurricane drills at every operating unit
- Power system restoration plans that are exercised to train operators and prepare all participants to clarify roles and responsibilities
- Participation in national exercises to ensure local emergency response plans are coordinated with the National Response Framework and the National Incident Management System

Rapid Recovery: Emergency Response

The electric grid is designed around the inevitability of localized failure, and each utility prepares for rapid response and recovery based upon its size and risks associated with the geographic location of assets. Emergency response and recovery is not a contingency plan, but an integral aspect of electric grid operation. One CEO identified the following key enablers of rapid recovery:

- Drills—real-time and simulated
- Design for redundancy
- Maintaining adequate spares
- Voluntary and formal mutual assistance agreements with other utilities

While regions prepare to the extent possible for known regional risks, severe and historic natural disasters are hardly expected. They are difficult to prepare for and greatly stress the response and recovery capabilities of local electric utilities, as shown by the Nashville floods in 2010 (see Exhibit 4.6).

Response and recovery in the face of both known hazards and possibly severe events requires robust preparation, plans, and procedures. The Study Group compiled an extensive exemplary list of response and recovery practices, which can be found in its entirety in Appendix B. The following are highlighted practices executives said they engage to enable rapid and effective recovery:

- As weather conditions change, companies alert their vendors, stock up on supplies, and ready response crews. Though it can cost more, one utility representative said the company pre-positions crews and supervisors in strategic geographic areas to enable faster response.
- Companies with their own on-site construction and repair personnel place them on standby. Other utilities begin working with contract services to place them on alert. One executive said his utility keeps a list of recently retired personnel on hand who could be mobilized to help. Another reported that the company uses 600–800 on-site personnel without outsourcing.
- Utilities work with vendors to pre-package special kits containing emergency spares and other equipment, and ready them at utility warehouses for quick distribution if needed.
- Pre-engineering plans for replacements are enacted and personnel begin preparing backup areas for installation.
- Formal and informal mutual aid agreements, pre-arranged with neighboring utilities and vendors, are put on operational alert. Mutual assistance agreements, generally organized regionally within the United States, are put into effect.
- Many companies build a surplus inventory of critical supplies and equipment in the event that replacements are inaccessible. An executive at a smaller utility said it maintains a $12 million inventory, while a larger company has its own warehouse of supplies with $40–$50 million in parts.
- Many utilities keep mobile spare transformers on hand and pre-deploy them in some circumstances. One representative of a large utility said the company maintains 12 single-phase transformers that exhibit a simple, mobile design.
- If available, utilities engage mobile offices or system-wide storm centers across the region. One executive said it deploys response personnel with trucks stocked with extensive communications technology, while others engage contractors embedded in the area rather than employees.

- Utilities meet with local authorities to coordinate response and recovery, activate emergency response plans, and turn on communication links to ensure the continuous flow of information.

Exhibit 4.6 Nashville Flooding of 2010

Event Summary

Following two days of torrential rains in May 2010, areas of middle and west Tennessee, south central and western Kentucky, and northern Mississippi experienced "1,000-year" floods that caused 31 deaths and an estimated $1.5 billion in property damage in the Nashville area alone. Rain totals exceeded 19 inches in some areas. The Cumberland River crested at 51.86 feet in Nashville, a level not seen since 1937, before the U.S. Army Corps of Engineers flood control measures were put in place. The Federal government declared 42 counties disaster areas.

Impacts

More than 150 roads were shut down including 50 in Davidson County alone. Southwest Airlines cancelled all of its flights. Public school systems in Davidson and surrounding counties cancelled classes. Hospitals delayed elective surgeries and the Metro transit shut down bus services. The Metro Water Service, one of two water treatment plants, shut down and residents were asked to conserve and use water only when necessary.

About 36,000 Nashville Electric Service (NES) customers in Davidson were without power, with 16 power lines and 20 poles down countywide. Flooding at an NES substation caused power to go out in the center of Nashville. Among the buildings that lost electricity was the 617-foot AT&T Building, the tallest building in Tennessee. Several substations were flooded; one was under 10 feet of water. Several high-voltage transmission towers collapsed into the river.

Response and Recovery

Crews had to use helicopters and air boats to inspect the sites because roads were washed out. Downtown streets were closed to allow NES to move employees and equipment such as poles and transformers to its downtown offices to facilitate the extensive flood restoration effort.

The extent of the flooding caused FEMA to redraw its flood plain for the area and led NES and the Tennessee Valley Authority to consider relocating transmission lines on the other side of nearby mountains away from the river and to place substations which could not be relocated on stilts or other structures to avoid flooding in the future.

Source: "Massive flooding hits Nashville," *Nashville Business Journal*; Tennessee Bar Association, "May 2010 Floods;" Tennessee Emergency Management Agency, "Bredesen Announces Disaster Declarations for 3 More Tennessee Counties;" Tennessean staff reports, "Obama declares Nashville a disaster area.;" U.S. Army Corps of Engineers, *After-Action Report.*

Major generation plants are also equipped with a rarely used but critical recovery capability for "black start" circumstances when power is completely out in a large region. These black start generators are able to start up without any external source of electric power and energize the transmission grid to bring power to generating plants that have completely shut down during a major system collapse. While energized, the grid is stable; when energy is lost during a cascading event, it becomes unstable and necessitates a deliberate and careful reintroduction of load into the system. Black start units are designed to bring back online major generation systems, such as nuclear power plants, that are the backbone of the bulk power system. As critical system components, black start generators fall under NERC reliability standards and they are tested periodically; many executives said that each plant has a black start plan and they regularly conduct drills for black start events. But concerns have been raised by about the age and condition of some units.

Adaptability: Incorporating Lessons Learned

As earlier discussed, integrating lessons learned from exercises, drills, and industry experience into operational practice is considered a responsibility of grid operators. Industry executives indicated that it is practice to hold follow-up meetings with emergency operations groups after every event to capture lessons learned. They then convene CEOs, other executives, and chief engineers to evaluate suggested enhancements and implement cost-effective reliability and resilience upgrades. Regular meetings with

neighboring companies, formally or informally, are used to share lessons learned and best practices, enabling one company's experience to improve resilience practices across the region or nation.

Companies take these experiences and feed them back into their operations, adapting planning scenarios and exercises to include new risks, adding redundancies or rebuilding using stronger and advanced equipment, and reconfiguring lines or assets to address a vulnerability uncovered by another entity. Individual company accountability is highly valued in the sector.

Exhibit 4.7 Florida Blackout of 2008

Event Summary

While diagnosing a malfunction on a circuit switcher at Florida Power and Light's (FPL) Flagami station on February 26, 2008, a protection and control engineer disabled the primary and secondary breaker failure protection without alerting the load dispatcher or system operator on duty—an action in conflict with existing documented maintenance practices. At the request of the engineer, the load dispatcher then opened the circuit switcher, whose bottle interrupter failed and caused a fault on the system that spread to the adjacent shunt reactor's circuit switcher, which in turn caused a three-phase fault on the 138 kV system. The disabled protections caused a delayed clearing of the transmission system fault—1.7 seconds—that led to significant frequency and voltage swings, and tripping of transmission and generation around portions of the lower two-thirds of Florida.

Impacts and Recovery

The event led to the opening of 22 transmission lines, 4,300 MW of generation, and 3,650 MW of customer service or load. Twin nuclear reactors in the Turkey Point Nuclear Generating Station and a fossil generation unit were shut down by designed equipment trips following severely depressed voltages. Approximately 596,000 Florida Power and Light (FPL) customer accounts and 354,000 non-FPL customer accounts were out of service, representing approximately 8% of Florida electric customer accounts. Despite the widespread impact of the operator error, the sector's preparation for unexpected events allowed a swift restoration of power; the event began at 1:08 p.m., and power was restored by 4:30 p.m.

Lessons Learned

FPL began implementing reliability enhancement measures immediately after the event and throughout a FERC investigation, including the following:

- Ensure better protection redundancy.
    - Implement protection redundancy for new transmission substations above 100 kV with in-service dates of 2010 and beyond, intended to ensure single points of failure on protection systems would not result in N-1 transmission system contingencies from evolving into more severe or extreme events.
    - Add high-speed redundant protection on the autotransformers at Flagami Substation.
    - Implement protection redundancy for the autotransformers at eight substations that have similar bus arrangements as Flagami.
- Ensure better alarm response.
    - Implement automatic remote monitoring of the protection circuit fuses and develop a procedure for immediate action in the case of an alarm.

The investigation resulted in a FERC order that FPL pay a civil penalty of $25 million and adopt seven reliability enhancement measures including training and certification, updated emergency response procedures, equipment maintenance, and frequency response maintenance. The Florida Reliability Coordinating Council conducted its own in-depth investigation that included seven parallel analyses resulting in 24 recommendations for all under the council that included implementing new tools and training procedures.

Source: FERC, "Order Approving Stipulation and Consent Agreement: Florida Blackout;" Florida Reliability Coordinating Council. *FRCC System Disturbance and Underfrequency Load Shedding Event Report*.

Notable events have created a drive for specific infrastructure improvements. The Northeast Blackout in 2003 and the Florida Blackout in 2008 highlighted, among other things, the need for more rapid recovery, better battery capabilities, and the need for repair and control operators to strictly adhere to standard operating procedures and communicate with each other (see Exhibit 4.7). Major floods in the South and other flooding events have led many in some areas of the country to put substations on stilts

and to move transmission on the opposite side of mountains to avoid river valleys. Icing in the Midwest has led utility companies to install dead-end transmission towers so that the collapse of one section of line is limited to a much shorter distance.

Major hurricanes such as Katrina, Rita, Floyd, and Isabel have exposed multiple gaps in electricity sector resilience. Following those events, many utilities discovered the need to keep cash on hand to pay employees unable to withdraw money from inoperable financial institutions and plan for the care of family members of key utility workers. Following Hurricane Floyd, utilities began expanding the number of customers anticipated to be without power in planning scenarios from 400,000 to 800,000. Utilities reported keeping extra Lindsey transmission towers on hand for quick emergency erection and drilling on-site wells to ensure that, if water is cut off at local pumping stations, the transformers and other critical equipment can still be cooled as required.

In an August 2010 study, the Department of Energy documented the extensive response of the energy industry to recent major hurricanes. Table 9 of that document, replicated in part in Exhibit 4.8, contains a summary of what it calls energy hardening and resilience activities undertaken by electricity transmission and distribution facilities in the surveyed southern States in response to recent hurricanes.

Exhibit 4.8 Summary Finding of *Hardening and Resiliency: U.S. Energy Industry Response to Recent Hurricane Seasons* [13]

Flood Protection
• Elevating substations/control rooms/pump stations • Relocating/constructing new lines and facilities
Wind Protection
• Upgrading damaged poles and structures • Burying power lines underground • Strengthening poles with guy wires
Modernization
• Deploying sensors and control technology • Installing asset databases/tools
General Readiness
• Conducting hurricane preparedness planning and training • Complying with inspection protocol • Managing vegetation • Participating in mutual assistance groups • Procuring spare T&D equipment • Purchasing or leasing mobile transformers and substations
Storm-Specific Readiness
• Facilitating employee evacuation and reentry • Securing emergency fuel contracts • Supplying logistics to staging areas

[13] DOE, *Hardening and Resiliency: U.S. Energy Industry Response to Recent Hurricane Seasons*.

Increasing Resilience through Leadership and Partnership

The grid—growing larger, increasingly digital, ever more intelligent and advanced—is at a critical juncture. The same electricity sector that has mastered reliability through risk management and made resilience an operational practice is now being asked to prepare for risks well outside of its experience, understanding, and traditional responsibilities. Coordinated attacks, pandemics, electromagnetic disturbances, terrorism, and severe natural disasters introduce the potential for widespread or lengthy outages at a time when the U.S. relies more than ever on uninterrupted power. The lines between providing reliable electricity and ensuring national safety and security begin to blur, responsibilities start to merge—and the imperative becomes clear: executives from government and industry must step forward in this area of joint responsibility and coordinate their efforts. Both have a role to play.

During this NIAC effort, the Study Group participated in a CEO Roundtable on July 14, 2010, hosted by Constellation Energy, to address the gaps and vulnerabilities identified in the BGE stress exercise of June 22. What the Roundtable found was the need for a process to discuss and share risks between the public and private sectors in areas of resilience that industry can't serve on its own. Two major suggestions for this process were made:

- The sector should develop its own sector-wide emergency response plan (ERP) for major disasters that would go beyond existing plans. This private sector ERP would outline structured communications and coordination protocols before an incident, identify key points of contact and decisionmakers in industry and government, clarify the triggers for various levels of response to different scenarios, establish priorities for recovery, and outline roles and responsibilities. All of this would be done within the context of current industry plans and the Federal government's National Response Framework and National Incident Management System.
- The sector should create a high-level process and mechanism for government and industry dialogue on ways to improve sector resilience. This process, building upon the existing public-private partnership model of the *National Infrastructure Protection Plan*, would establish a mechanism by which industry CEOs could consult with counterpart executives in government to work out solutions. The CIKR Executive Industry Council (EIC) proposal, implemented in response to a major theme from the 2009 NIAC study on *Critical Infrastructure Resilience*,[14] was identified as an appropriate mechanism for this dialogue.

Technical and Operational Measures to Increase Resilience

Interviews and discussions revealed that executives have already identified numerous technical and operational improvements that represent short-term activities utilities can take to realize significant resilience improvements, including: building in more redundancy, replacing aging with more modern equipment, designing to higher standards, and increasing the number of spares on hand. Additional examples our study identified include:

- Building more robust transmission systems
- Improving cyber security coordination with Federal agencies
- Adopting new risk assessment tools, such as probabilistic models used by the nuclear sector
- Planning to a higher level of reliability by building beyond N-1
- Planning to higher resilience standards to mitigate the effects of HILF events

[14] See especially Recommendation 4 and supporting discussion from NIAC, *Critical Infrastructure Resilience: Final Report and Recommendations*.

- Reducing the vulnerability of high-voltage transformers by acquiring more spares, standardizing design specifications, and encouraging domestic manufacturing
- Increasing the number of interconnections and transmission lines to reduce congestion on the grid
- Establishing better relationships with emergency response agencies before major events occur
- Achieving better understanding of non-conventional risks and how best to respond to them
- Deploying digital technologies to make the grid smarter and improve reliability

Though utilities know how to improve resilience, each of these activities comes at a substantial cost, and none offers a silver bullet solution to greater resilience in the sector. Utilities are frequently stalled from taking action because emerging electricity sector risks are difficult to quantify, making the high cost of improvements to address those risks difficult to justify in a regulated market. Large infrastructure changes, such as building more transmission lines and interconnections, require rights-of-way approval from local communities and public utility commissions, as well as the Federal government in some instances. The application process takes years and approval is not always forthcoming.

These represent areas in which effective public-private collaboration could accelerate progress with the sector. Improving electricity sector resilience is possible and needed, but will require public-private coordination on a national level to enact improvements beyond what the private sector presently has planned.

Government Has a Clear Role

Both the public and private sector have key roles to play in enhancing the resilience of the electricity sector. What follows are activities where government leadership can make a significant impact:

- Align Federal, State, and local governments in policy, planning, standards, and regulations.
- Establish single points of contact and authority to coordinate with utilities during emergency events.
- Expedite mutual assistance programs regionally, nationally, and internationally.
- Ensure fair cost recovery.
- Enable the movement of sector assets during emergencies.
- Provide safe and secure warehousing for hard-to-replace components such as high-voltage transformers.
- Improve access to government information regarding cyber threats and risks.
- Define and communicate government accountability, responsibility, and roles.
- Establish within the Federal government a single contact person on key issues such as cyber security and make that known to industry.
- Avoid establishing single or common solutions to resilience in the electricity sector; the sector is too complex, diverse, and geographically dispersed to accommodate this approach.

Electricity sector CEOs and managers are willing and ready to engage in a meaningful, executive-level partnership with the U.S. government. It is time to delineate roles, clarify responsibilities, and take action on addressing resilience needs and defining goals and activities for all stakeholders.

Sector Goals

In the course of our executive interviews, research, and discussions, the Study Group could not identify an agreed-upon set of outcome-focused resilience goals for the electricity sector. However, we did identify goals within sector organizations that encompass many of the strategies to achieve resilience that are closely aligned with findings and recommendations contained in this report.

The Electricity Sub-Sector Coordinating Council (ESCC) is a component of the public-private partnership to secure critical infrastructure. It represents the interests of electricity sector owners and operators to "foster and facilitate the coordination of sector-wide policy-related activities and initiatives to improve the reliability and resilience of the electricity sector, including physical and cyber security infrastructure." The ESCC has recently developed a draft vision statement and six goals that articulate its strategy to secure the electricity infrastructure, shown in Exhibit 4.9.

Exhibit 4.9 ESCC Vision Statement and Goals

Vision

The Electricity Sub-Sector envisions a robust, resilient electricity infrastructure in which continuity of business and services are maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between sub-sector entities and government.

Goals

Information Sharing and Communication

1. Establish robust situational awareness within the electricity sub-sector and with government through timely, reliable, and secure information exchange.

Physical and Cyber Security

2. Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resilience.

Coordination and Planning

3. Conduct comprehensive emergency, disaster, and business continuity planning, including training and exercises, to enhance reliability and emergency response.
4. Clearly define critical infrastructure protection roles and responsibilities.
5. Understand key interdependencies and collaborate with other critical infrastructure sectors to address them, and incorporate that knowledge in planning and operations.

Public and Regulatory Confidence

6. Strengthen public and government regulatory agency confidence in the subsector's ability to manage risk and implement effective security, reliability, and recovery efforts.

Source: NERC and the Electricity Sub-Sector Coordinating Council, *Critical Infrastructure Strategic Roadmap (DRAFT).*

Resilience is a core element of the ESCC's vision. It builds on the belief that trusted public-private relationships, information sharing, and effective risk management will result in robust and resilient electricity infrastructures. The six goals support this vision through information sharing and communication, physical and cyber security, coordination and planning, and public and regulatory confidence.

Although the Study Group did not attempt to set sector goals, the practices we identified suggest an implied set of outcome-focused resilience goals. They are:

1) Withstand a shock from any hazard with no loss of critical functions.

2) Prevent a power disruption from cascading into interconnected systems.
3) Minimize the duration and magnitude of power outages through rapid recovery strategies.
4) Mitigate future risks by incorporating lessons from past disruptions, simulations and exercises, and sound risk assessment processes.

These prospective goals were used to help develop the framework for establishing resilience goals described in Section 3.

4.2 Resilience in the Nuclear Sector

Nuclear power plants are exhaustively engineered and designed to withstand almost all conceivable manmade and natural hazards, short of an act of war. Protection and resilience are built into the design and operation of the facility. Additional layers of protection and resilience are added when credible new threats are identified. This section summarizes key information on sector design, regulation, interdependencies, and resilience practices garnered through discussion with the Nuclear Energy Institute; a more extensive case study can be found in Appendix C.

Assets and Infrastructure

Nuclear energy provides about 20 percent of the electricity in the United States through 104 reactors in 65 nuclear power plants located in 31 States. There are 32 companies licensed to operate nuclear reactors (referred to as licensees). Most reactors function at more than 90 percent capacity; once fueled, nuclear reactors can operate continuously for about two years.[15]

Regulation

The U.S. Nuclear Regulatory Commission (NRC) was created as an independent agency by Congress in 1974 to enable the Nation to safely use radioactive materials for beneficial civilian purposes. The NRC regulates commercial nuclear power plants and other uses of nuclear materials, such as nuclear medicine, waste, and the entire fuel cycle, through licensing, inspection and enforcement of its requirements.

Security regulations are based on a "design basis threat," which is characterized as a suicidal, well-trained paramilitary force, armed with automatic weapons and explosives, and intent on forcing its way into a nuclear power plant to commit radiological sabotage. The design basis threat is reviewed annually and updated as new intelligence and law enforcement information comes into the NRC.

Interdependencies

Nuclear sector interdependencies primarily include the electricity, IT, and telecommunications sectors. Lacking power storage, power plants must immediately channel electricity to transmission lines; if all lines to a nuclear power plant are down, the plant must go to cold shutdown for safety purposes. The electricity sector in turn depends on the nuclear sector for reliable electricity. Information technology and telecommunications provide the systems and networks that enable critical processes and communications.

Risk Profile

The nuclear power industry has decades of experience in physical security and emergency preparedness. Nuclear power facilities face risks from natural disasters, accidents, terrorist attack, and internal sabotage. The cyber security of critical control systems is emerging as a growing risk. Risks to nuclear and radiological materials include theft, diversion from intended use, and supply chain disruption, including interruption to the proper end-of-life disposal of nuclear and radiological waste.

If one or more reactors were to shut down for any reason, the electric grid itself would not be damaged. Of much greater concern is the unauthorized access to, use, or release of nuclear and radiological material, which could cause significant loss of life, economic disruption, and social-psychological impact.

[15] Nuclear Energy Institute, "U.S. Nuclear Power Plants: General Statistical Information."

The nuclear sector is designed and operated to mitigate these risks and to rapidly respond to and recover from any incident.

Resilient Practices

The nuclear sector emphasizes defense in depth, redundancy, and mitigation analysis. Although details are not publicly available, security procedures are exceedingly robust, layered, and exercised. The Nuclear Regulatory Commission (NRC) has extensive regulations that industry must follow in regards to both physical security and emergency preparedness.

Robustness

Nuclear plant security zones are given increasingly robust layers of access control and protection. The reactors themselves are steel-reinforced concrete structures made to withstand earthquakes, hurricanes, tornadoes, and floods. Exhaustive analysis by NRC determined that an airplane attack on a nuclear power plant would be unlikely to affect public health and safety, and the Electric Power Research Institute confirmed that the primary structures of a nuclear plant would withstand the impact of a wide-body commercial airliner.[16]

Additional physical security measures include extended and fortified security perimeters, barriers and illuminated detection zones, well-trained and armed security officers on duty 24/7, surveillance and patrols, intrusion detection devices such as high-tech surveillance equipment, bullet-resistant barriers to critical areas, vehicle and personal search procedures, barriers to protect against vehicle bombs, multiple access control points, a dedicated contingency response force, and force-on-force training exercises to evaluate security officer response to mock adversary attacks. Site security forces coordinate closely with external law enforcement.

Cyber security measures include isolation of control system computers from the Internet; the industry-wide implementation of cyber security guidelines developed in cooperation with the Pacific Northwest National Laboratory; NRC approval of plant cyber security plans to ensure the capability for timely detection, response, and mitigation of cyber attacks; the correction of exploited vulnerabilities and system restoration; and ongoing assessments and quarterly DHS briefs on new cyber security threats.

Personnel security measures include enhanced psychological assessments, fingerprinting, and background checks for employees; information sharing on personnel between reactor licensees; access controls; insider threat mitigation programs; repeated drills and testing of attempted sabotage; and biometric and other identification to enter sensitive areas.

Resourcefulness

Among the regulations governing nuclear power plant emergency preparedness are 16 planning standards (or capabilities), two emergency planning zones (10-mile plume exposure pathway and 50-mile ingestion exposure pathway), and annual letters of certification for State and local plans. The 16 planning standards are established by NRC and the Federal Emergency Management Agency (FEMA) and include such capabilities as on-site emergency response organizations, notification methods, emergency communications, accident assessment, protective response, radiological exposure control, recovery and reentry, and exercises and drills.

[16] U.S. Nuclear Regulatory Commission, “Security Spotlight;” Electric Power Research Institute, “Deterring Terrorism: Aircraft Crash Impact Analyses Demonstrate Nuclear Power Plant’s Structural Strength.”

In addition, the industry adheres to a standardized, four-level emergency classification system, ranging from notification of unusual events to general emergency. Both on-site and offsite response plans contain detailed guidelines for each emergency classification level. Notification procedures also are regulated, routinely exercised, and have dedicated secure communications systems in place with backups.

Rapid Recovery

Training, drills, and evaluated exercises are an important part of the sector's emergency preparedness. On-site staff are trained and re-qualified annually, and emergency drills are held quarterly. Offsite response organizations also have annual training programs and certification, as well as drills and exercises.

Adaptability

Beyond preparedness and response drills, the nuclear sector is proactive in improving the security of its nuclear power plants and other sector elements. All plants participate in the DHS Comprehensive Review (CR) process and voluntary enhancements to power plant security are tracked through the Comprehensive Review Outcomes Working Network (CROWN). All U.S. organizations that operate commercial nuclear power plants are members of the Institute of Nuclear Power Operations, established in 1979 to help the nuclear power industry achieve the highest levels of safety and reliability. Improvement in industry security is further facilitated through an active program of lessons learned in which NEI members of the Nuclear Strategic Issues Advisory Committee (NSIAC) consider enhancements to security and vote on which to implement industry wide.

Leadership and Partnership

The nuclear sector maintains a close relationship to the Federal government, which it partners with on security-related research and development. The Department of Energy and its associated national laboratories maintain a vigorous program of activities related to security in the nuclear sector. These programs include research and development focused on advanced methods for manufacturing and construction, risk assessment methods, improved instrumentation and controls, and high-performance modeling and simulation.

5.0 Findings

A core principle of our homeland security strategy is that it is a shared responsibility of the private sector, government, communities, and individuals. This is particularly true for critical infrastructures: they are mostly built, owned, and operated by the private sector; their services and products are used by businesses, individuals, communities, and government; and their public safety and economic stability is ensured by government regulation and oversight. We must creatively engage and integrate the capabilities of all these partners to ensure the resilience of our Nation's critical infrastructures.

The continuity of critical infrastructures is a key objective for the private and public sectors. Private sector companies devote extensive resources to ensure uninterrupted service to customers, protect shareholder interests, fulfill fiduciary responsibilities, and protect investment in corporate assets. In the electricity sector, millions of dollars and hours are devoted to minimizing the impact of outages and preparing for all types of disasters: natural events, accidents, and malicious attacks. For the government, the continuity of operations in these infrastructures—and electric power in particular—is critical to many of its fundamental missions: economic stability and growth, national security, public safety, and quality of life. In the new security environment, the private sector needs a strong partnership with government to get the best threat information up front and as a disaster unfolds so it can provide the high level of resilience that customers need and expect. While all partners have a stake in the continuity of critical services and functions, the private sector and the local communities they serve are the partners on the ground during a crisis. However, all too often, the government policies and regulations overlook, rather than integrate, the best private sector practices, processes, and people to ensure infrastructure continuity.

The Council believes that public-private partnership is the fundamental strategy to ensure the protection and resilience of our critical infrastructures. To quote our previous study on the partnership, *"It represents the best long-term strategy to secure our critical infrastructures, in contrast to regulatory approaches that are less efficient, are less effective, and create antagonism between public and private sector entities that must cooperate to succeed."*[17] The *National Security Strategy*, released by the White House in May 2010, not only recognizes the importance of infrastructure resilience to national security but also reinforces the role that public-private partnerships play in improving resilience (see Exhibit 5.1).

Exhibit 5.1 Improve Resilience Through Increased Public-Private Partnerships

When incidents occur, we must show resilience by maintaining critical operations and functions, returning to our normal life, and learning from disasters so that their lessons can be translated into pragmatic changes when necessary. The private sector, which owns and operates most of the Nation's critical infrastructure, plays a vital role in preparing for and recovering from disasters. We must, therefore, strengthen public-private partnerships by developing incentives for government and the private sector to design structures and systems that can withstand disruptions and mitigate associated consequences, ensure redundant systems where necessary to maintain the ability to operate, decentralize critical operations to reduce our vulnerability to single points of disruption, develop and test continuity plans to ensure the ability to restore critical capabilities, and invest in improvements and maintenance of existing infrastructure.

Source: White House, *National Security Strategy,* 19.

An important context of our findings and recommendations is that *shared responsibility* does not necessarily mean the *same responsibility* or *historical responsibility*. Our case studies of the electricity and nuclear sectors highlighted the distinct functions and unique capabilities of the private sector in designing, building, operating, and maintaining increasingly complex infrastructures. The government helps to strengthen and sustain these functions by sharing risk information, providing a reinforcing regulatory environment, creating needed incentives to spur investment, and providing key resources

[17] NIAC, *Critical Infrastructure Partnership Strategic Assessment*, 5.

during extreme disasters when the capabilities of the private sector are exceeded. The case studies also revealed how the changing risk landscape is causing the private sector to rethink the traditional boundaries of service providers, customers, communities, and government in ensuring the reliability and resilience of the electricity and nuclear sectors. The following findings and recommendations are predicated on the belief that the partnership approach can unite the special capabilities and expertise of the public and private sectors to minimize infrastructure risks and improve resilience.

Resilience in the Electricity and Nuclear Sectors

1. **The U.S. electricity and nuclear sectors are highly reliable and resilient. However, the scope and depth of the resilience practices used routinely by these sectors are not well understood or communicated.** The North American bulk power system is designed and operated to absorb shocks, avoid cascading failures, and recover rapidly. This is enabled by rigorous planning, construction, and operating requirements; an interconnected, high-voltage, bulk power system in which generation and transmission is dynamically managed in a highly structured way; and a strong culture of commitment to reliability and mutual assistance. The local power distribution system is also highly reliable and has a history of rapid restoration after outages, drawing upon resources from other utilities when outages are widespread. The sectors' track record of reliability and resilience is based in part on their ability to skillfully integrate lessons learned from past power outages.

   Our study found hundreds of examples of how power utilities mitigate risks in day-to-day operations using advanced technology, planning processes, recovery practices, supply chain management, company organization, personnel training, and system architecture. Many of these practices are so ingrained in the operations and culture of the utility industry that many within the industry do not label them as resilience, but rather as core reliability principles, necessary safety features, or sound business practices. Some outside the industry may believe that electricity sector resilience means that the lights never go out, and may be unaware of the extensive resources expended to minimize all-hazard risks. A lack of knowledge of power system operations and the absence of a common language of resilience create a gap in understanding throughout industry and government about resilience.

   Other CIKR sectors may be similarly challenged in explaining and communicating the significance of their business and resilience practices. For example, a previous NIAC study gave an example of a misunderstanding between telecommunication companies and banking and financial companies regarding a separate, redundant backup communication system that failed during the September 11th attacks because it required a manual switchover at a Verizon building that was damaged when the 7 World Trade Center building collapsed. Gaps in the terminology and understanding of resilience can be significant when designing government programs and policies aimed at enhancing resilience in specific critical infrastructures.

2. **Electricity and nuclear sector practices suggest an implied set of sector goals based on the framework for resilience.** The large number and variety of utility practices, strategies, and actions suggest several underlying resilience goals that the electricity and nuclear sectors have already adopted. These include: 1) Withstand a shock from any hazard with no loss of critical functions; 2) Prevent a power disruption from cascading into interconnected systems; 3) Minimize the duration and magnitude of power outages through rapid recovery strategies; and 4) Mitigate future risks by incorporating lessons from past disruptions, simulations and exercises, and sound risk assessment processes.

Utilities harden assets and build in redundancy where it makes economic sense based on likely risk, cost, and impact. However, protecting against all risks to the electric grid is costly and impractical. That is why rapid recovery is often the most cost-effective and flexible resilience strategy for the electricity sector. A strong capability for rapid recovery—enabled by training and drills, pre-positioned supplies, vendor and contractor relationships, mutual aid agreements, and past experience—often provides a more flexible resilience strategy because it can respond to failures regardless of the cause (weather, equipment failure, accidents, malicious events, etc.).

The Emerging Risk Landscape

3. **The risk landscape is changing in ways that may affect both the reliability and resilience of the electric power sector.** Nearly every industry executive gave examples of how extreme weather events, such as Hurricane Katrina, forced a reassessment of emergency practices, business continuity plans, and system design. The ability to incorporate new lessons from past outages is a hallmark of the power sector and a key strategy in mitigating future risks. However, on the horizon are a number of other emerging unconventional risks and threats that will challenge the capacity of the industry to "power" the nation. These include targeted physical and cyber attacks, electromagnetic pulses and geomagnetic disturbances, growing interdependencies with other critical infrastructures (notably telecommunications and fuels), and the potential of a pandemic. Many of these risks will require actions that are beyond the purview of a single company or even the entire industry, and will require collaborative foresight exercises and shared responsibility and investment. The changing risk landscape magnifies the need for partnerships across CIKR sectors and between the public and private sectors. However, new responses to emerging risks must be rooted in industry's best practices and processes—and the companies themselves should have principal authority to implement and execute these new responses.

   The nature of the electricity system is also in the midst of important change. Customer requirements and new regulations are changing the way electricity is produced and managed; renewable resources that have different load characteristics are being added to the electric grid; historical generation and load centers are changing; utilities are increasing their use of digital devices to monitor and control electricity; and businesses and consumers are using electricity to power a host of new devices from hand-held electronics to automobiles. These changes are placing new demands on the electric grid that could affect the reliability, stability, and integrity of the system.

4. **Increased cyber monitoring and control of the electric grid has reshaped risks in ways that are not fully understood.** The increased use of cyber-based control systems to manage transmission and distribution has increased system functionality and reliability, but has also introduced new risks in the electric grid. Energy management systems and supervisory control and data acquisition (SCADA) systems that share common infrastructure or connect to business systems may expose the electric grid to cyber intrusions. The development of the smart grid and the introduction of new digital control equipment offer additional opportunities for system control and security, but also create the potential for millions of new points of entry for malicious attacks. Federally-mandated cyber security standards are now in place for the bulk power grid. However, Federal agency responsibility regarding cyber vulnerabilities, information sharing, emergencies, and mitigations are still unclear to many utilities. In addition, the difficulty in assessing cyber risks may be creating a culture of compliance at the expense of a culture of security.

5. **Cross-sector risks faced by the electricity sector include fuel supply, telecommunications and IT, transportation, and water.** As one of the “lifeline sectors,” the power sector is expected to operate when other infrastructures are out of service, and it does this quite well. Electric and nuclear utilities

must be prepared to operate and rapidly recover during hurricanes, ice storms, or floods, even if the sectors they rely on are down. Yet the power sector is far from independent; it relies on fuel supplies to power generators; water for cooling; data networks to operate control systems that manage power throughout the electricity system; telecommunication systems to contact emergency personnel; and transportation networks to deliver fuel, equipment, and personnel. For each of these dependencies, the sector has developed significant redundant systems and alternatives. These include on-site fuel storage facilities, private fiber optic networks, radio and satellite communications, and alternative vendors for supplies and repair equipment.

Challenges and Opportunities to Increasing Resilience

6. **The limited availability of extra-high-voltage transformers in crisis situations presents a potential supply chain vulnerability.** Although utilities are quite adept at managing their equipment inventories and supply chains, extra-high-voltage transformers in particular may present a weak link in the sector's resilience. These transformers are highly specialized equipment, have 18- to 24-month manufacturing lead times, and are difficult to transport. Their high cost limits the ability of utilities to maintain many spares, which are often co-located at substations, thereby increasing their vulnerability. Industry programs to share spares help to mitigate risks, but the application of this arrangement has been limited in practice and widespread application is untested.

7. **The ability of utilities to achieve greater levels of resilience is constrained by market, regulatory, and technical factors.** The electricity sector is very capital-intensive and highly regulated by Federal and State commissions. Long-lived capital assets means that equipment and infrastructure turn over slowly while the risk landscape is changing rapidly. Investments in reliability and resilience beyond those required by existing regulations must be justified as benefiting the customers who will ultimately have to pay for them. In addition, the ability of the industry to increase resilience by expanding transmission lines to relieve congested corridors and build better interconnections is constrained by the difficulty in obtaining access to new rights-of-way. Further, electricity is a "millisecond" industry and it must be delivered instantaneously; there are few cost-effective options for bulk storage.

8. **Government information sharing on risks to the electricity sector has improved, but more can be done.** There is growing evidence that the sharing of threat and risk information by the government with the private sector has improved. However, power companies still believe they are not receiving timely, actionable information to effectively manage certain types of risks. Key barriers include the difficulty in translating classified threat information into non-classified, actionable information and the limited number of clearances within utilities needed to receive classified information. For example, a recent GAO survey indicated that 98 percent of private sector respondents expects timely and actionable cyber threat information, but only 27 percent indicated it is being adequately provided by Federal partners.

9. **Restoration planning, including black start capabilities, provides an effective measure of recovery but deserves more focused attention.** Despite excellent reliability and efficient rapid recovery capabilities, the electricity industry recognizes the risk of blackouts. Restoration planning for large-scale outages includes the contingency for a "black start" in which generation must be brought back online and the grid restored without connected power sources. Although the industry regularly conducts live tests and exercises for this low-probability event, additional planning, through current authorities such as independent system operators, regional transmission operators, and the North American Electric Reliability Corporation, may be warranted under certain scenarios.

10. **Boards of directors at power companies receive a high volume of risk information, but it remains difficult to communicate and quantify operational risks in a rapidly changing risk environment.** Boards today are operating in one of the most challenging business environments ever encountered; the rapid speed of change and the complexity of emerging risks means that boards have little lead time to identify approaching opportunities or changes and provide proper oversight. Emerging operational risks are difficult to quantify and balance with a traditional risk profile, making the efficient communication of potential impacts a challenge. The availability, quality, timeliness, and format of risk information will impact the board's ability to provide meaningful oversight. Increasing Federal initiatives and regulations aimed at mitigating operational risks diminish oversight power of the board of directors and introduce another layer of compliance concerns. Additionally, emerging operational risks—including more complex technologies, terrorism, pandemics, and cyber threats—are increasingly interrelated, placing a higher importance on interdependencies—and these risks increasingly affect financial performance.

    Boards see gaps in their oversight capabilities where the company has not assigned sufficient resources to its risk management system, or where the roles of the full board and its standing committees are undefined with regard to risk oversight. Appropriate resources and defined roles enable the board to examine individual risks throughout the organization, collaborate between risk specialties, and anticipate emerging or interacting risks. Periodic review of the board's risk oversight process, and monitoring the alignment of the organization's strategy against emerging risks, regulations, and incentives, will better enable the board to achieve its oversight objectives.

6.o Recommendations

1. **The White House should initiate an executive-level dialogue with electricity and nuclear sector CEOs on the respective roles and responsibilities of the private and public sectors in addressing high-impact infrastructure risks and potential threats, using an established private sector forum for high-level, trusted discussions between industry executives and government leaders.** Senior public and private sector leaders need to better define and understand their respective roles and responsibilities in preparing for and recovering from major events, including high-impact, low-frequency events. The public-private partnership model, as implemented through the Critical Infrastructure Partnership Advisory Council (CIPAC), provides an effective mechanism for coordinating the shared responsibility of infrastructure resilience. It establishes an excellent structure for planning and implementation by bringing much-needed functional expertise to the table. However, most of the participating individuals are not empowered to make decisions for other parts of their organization or do not have the ability to influence CEOs throughout the sector on priority issues. As the NIAC recommended in its report, *Critical Infrastructure Partnership Strategic Assessment,* the partnership model needs to engage private sector CEOs with their counterparts in government using a scalable sector model. The NIAC reaffirms this recommendation and calls for a new public-private dialogue that uses an existing executive-level forum of private sector CEOs and their government counterparts to focus on high-level policy issues; create a framework for public-private collaboration with defined roles and responsibilities; and make recommendations that strengthen overall resilience, especially for high-impact, low-frequency risks.

Exhibit 6.1 Lessons Learned from the Gulf Oil Spill

"You have to generate unity of effort because there are overlapping roles, jurisdictions, competencies, authorities. And what you want to do is bring that together and focus it on the effects you're trying to achieve. I would say that is the single most important common denominator in any emergency response. "

"I think what we're finding out, whether it's a hurricane or an oil spill, there's always going to be a gap between what you're legally allowed to do and what the country expects. And I think moving forward, if we really wanted to think about it, we need to understand what to do with that government effort that's expected by the public that's not covered by a law."

—U.S. Coast Guard Admiral (ret.) Thad Allen
Interviewed on National Public Radio, September 9, 2010

2. **The nuclear and electricity industry should each develop an emergency response plan that outlines a coordinated industry-wide response and recovery framework for a major nationwide disaster.** Although electric and nuclear utilities have robust emergency response plans and exercise them regularly, there is no industry-wide plan to address a major national disaster. While relationships between the companies and their States, regions, and communities are well established, the relationships, roles, and responsibilities at the national level are less clear. The Council recommends that coordination and development of such an emergency response plan be led by CEOs in each sector and aligned with the National Response Framework and National Incident Management System. The plan should identify the types of disasters that will activate the plan and identify who makes this decision; clarify roles and responsibilities within the electricity industry and between various public and private sectors for specific functions; set priorities and the actions that will take place once decisions are made; describe expectations of Federal and State governments for certain types of disasters; and provide a structured communication plan with appropriate protocols.

   NIAC recommends that the responsibility to coordinate and develop such an emergency response plan be determined by the leadership of each sector. However, existing organizations, such as the CEO Business Continuity Task Force of the Electric Edison Institute (EEI) could lead this effort within the electricity sector, in coordination with North American Electric Reliability Corporation (NERC),

the American Public Power Association, and the National Rural Electric Cooperative Association. The Nuclear Energy Institute could lead this effort within the nuclear industry.

3. **DHS and other Federal agencies should improve information sharing with the private sector by providing focused, actionable, open-source information on infrastructure threats and vulnerabilities.** While some information can only be shared in a classified setting, many of the useful incidents and trends can be culled from open sources and distilled into actionable recommendations to the private sector. The NIAC heard several examples of executives who gained key insights from analysis of open-source information that was tailored to their sector. DHS and other Sector-Specific Agencies should work with their private sector counterparts through the CIPAC structure to identify the types of information that would be most valuable to owners and operators and the best mechanism to deliver it to them. DHS and other government agencies should develop more effective ways to share classified content with the electricity and nuclear sectors, or translate it into useful non-classified information.

4. **All critical infrastructure sectors should consider adopting the industry self-governance model exemplified by the Institute of Nuclear Power Operations (INPO) and the North American Transmission Forum (NATF) to enable the private sector to collaborate on industry-wide resilience and security issues outside the regulatory compliance process.** The nuclear industry created INPO as a private organization to address critical safety and reliability issues in the aftermath of the Three Mile Island disaster. Its defining feature is a self-governing model that commits each company to achieve excellence in nuclear power plant operations. This is backed up by plant evaluations that are shared within the nuclear sector in an honest and trusted environment, but outside the regulatory process. The INPO model is effective because it enables better use of industry resources by sharing the solution and not just the problem.

   More recently, the NATF has adopted this model to address transmission reliability and resilience issues across the electricity sector in the aftermath of the 2003 Northeast blackout. Although both organizations were established in response to specific sector problems, their value to improving overall accountability, communication, and performance across their sectors is clear. Such industry organizations can provide regular evaluation of the resilience and security of sector assets and systems, establish performance objectives, train and educate sector employees, and create CEO accountability for any shortcomings in performance. The self-monitoring nature of such an organization would not be a substitute for existing regulation, but would provide an extra measure of responsibility and care for overall industry performance.

5. **Promote the use of the NIAC-developed framework for setting resilience goals in the Critical Infrastructure and Key Resources (CIKR) sectors and for providing a common way to organize resilience strategies within Federal and State governments and CIKR sectors.** The goal-setting framework developed by the Council should be used to help critical infrastructure sectors discern their resilience goals. The process enables sectors to not only establish outcome-based goals but also uncover gaps in sector resilience and develop options to address them. The process establishes a baseline of current practices, develops high-level resilience goals, tests the sector's resilience in a high-impact scenario, and addresses gaps and seams through a public-private dialogue. The process is flexible enough to be used by all CIKR sectors despite their differences in assets, businesses, and risk profiles. DHS should consider using this resilience framework as a common way to organize resilience strategies and programs.

6. **DHS should support modeling and analysis studies of the cross-sector economic impacts of CIKR failures using tools such as input-output analysis.** Many of the CIKR sectors are highly

interconnected, which can improve resilience but also create new opportunities for problems to cascade across sectors, regions, and economic systems. Understanding the impact of sector failures is becoming more important as infrastructures become increasingly interconnected. The NIAC report, *Critical Infrastructure Partnership Strategic Assessment,* recommended that the government increase resources to conduct cross-sector studies and analysis, guided by private sector knowledge of infrastructure operations. The NIAC reaffirms this recommendation and highlights the need to place special emphasis on supporting studies that apply established economic models and tools to examine how increased interconnection affects infrastructure resilience and economic impacts.

7. **Federal and State agencies should allow cost recovery for utility investments that increase infrastructure resilience.** Utility investments in reliability and resilience beyond those required by existing regulations must be justified as benefiting the customers who will ultimately have to pay for them. To encourage the private sector to invest in the resilience of transmission and distribution systems, government agencies should modify their processes for allowing rate adjustments. For transmission systems, the Federal Energy Regulatory Commission (FERC) should initiate a rulemaking that enables utilities to recover costs of infrastructure investments that improve resilience. For distribution systems and some transmission systems as well, ratemaking is done by individual State PUCs. NIAC recommends that the National Association of Regulatory Utility Commissioners or another appropriate body issue policy recommendations to State utility commissions encouraging cost recovery for investments that improve resilience as part of their ratemaking process.

8. **Electricity industry and government leaders should pursue options to mitigate supply chain vulnerabilities associated with extra-high-voltage transformers.** Nearly everyone we spoke with recognized the supply challenges posed by extra-high-voltage transformers, including long manufacturing lead times, foreign production, large cost, highly customized designs, and difficult transportation logistics. Because maintaining spare transformers at all locations is extremely costly, the sector, through EEI, created a program that helps utilities to share their inventory of spare transformers and mitigate sector risks. However, the Council believes that additional steps are needed to further reduce supply chain risks.

   The Council recommends that the EEI Spare Transformer Equipment Program (STEP) be expanded and that EEI collaborate with NERC to determine the requirements for spare transformers for electric systems of various sizes. Domestic manufacturing of high-voltage transformers has begun to reemerge in the United States and several companies have recently opened facilities or announced new construction. Because of the important role that transformers have in maintaining sector reliability and resilience, the government should consider providing incentives to encourage additional domestic manufacturing of extra-high-voltage transformers if it is determined that this is needed to fortify national security objectives. Additional options, including standardization of transformer design and development of a recovery transformer, should be addressed as a priority issue by electricity sector CEOs and government executives through the executive-level dialogue outlined in Recommendation 1.

9. **The Federal government should work with owners and operators to clarify agency roles and responsibilities for cyber security in the electricity sector, including those for cyber emergencies and nation-state threats.** The Federal regulatory framework and roles for all stakeholders involved in securing the electric grid should be clear to avoid duplicative or conflicting actions in times of crisis. The electric utility industry is not in the law enforcement or intelligence gathering business, and the government has limited experience operating the electric grid. Thus, each should be consulted, and the flow of information should be regularly exercised, before a threat becomes a

crisis. To avoid confusion, those at the highest levels of government and industry should be involved in coordinating responses and declaring the need for emergency action. The electricity industry is also facing new highly sophisticated cyber threats, possibly from nation-states, that may exceed the capability and responsibility of owners and operators. The Council recommends that the White House work with electricity sector CEOs to clarify public and private roles and responsibilities in managing these cyber risks that could compromise the integrity of the bulk power system.

Appendix A About the NIAC

NIAC Members

Chair—Mr. Erle A. Nye, Chairman Emeritus, TXU Corp.

Vice Chair—Mr. Alfred R. Berkeley III, Chairman, Pipeline Trading Systems, LLC *(Vice Chairman (retired) NASDAQ)*

Mr. David J. Bronczek, President and CEO, FedEx Express

Mr. Wesley Bush, Chief Executive Officer and President, Northrop Grumman

Lt. Gen. Albert J. Edmonds (ret.), Chairman and Chief Executive Officer, Edmonds Enterprise Services, Inc.

Chief Gilbert L. Gallegos (ret.), Chief of Police, City of Albuquerque, New Mexico

Ms. Margaret E. Grayson, President, Grayson & Associates

Mr. Philip G. Heasley, President and CEO, ACI Worldwide

Commissioner Raymond W. Kelly, Police Commissioner, New York Police Department

Mr. David Kepler, Executive Vice President, Chief Sustainability Officer, Chief Information Officer, Dow Chemical

Mr. James B. Nicholson, President and CEO, PVS Chemical Inc.

Mr. Thomas E. Noonan, Former General Manager, IBM Internet Security Systems

Hon. Tim Pawlenty, Governor, State of Minnesota

Mr. Gregory A. Peters, Chief Executive Officer, News Distribution Network Inc.

Mr. James A. Reid, President, Eastern Division, CB Richard Ellis

Mr. Bruce Rohde, Chairman and Chief Executive Officer Emeritus, ConAgra Foods Inc.

Dr. Linwood H. Rose, President, James Madison University

Mr. Matthew K. Rose, Chairman, President and Chief Executive Officer, BNSF Railway Company

Mr. Mike Wallace, Vice-Chairman and COO, Constellation Energy; Chairman, UniStar Nuclear Energy; Chairman, Constellation Energy Nuclear Group

Mr. Greg Wells, Senior Vice-President—Operations, Southwest Airlines

Ms. Martha B. Wyrsch, President, Vestas Americas / Vestas Wind Systems, NA

About the NIAC

The National Infrastructure Advisory Council (NIAC) provides the President, through the Secretary of Homeland Security, with advice on the security of critical infrastructures, both physical and cyber, supporting sectors of the economy. The NIAC also advises the lead Federal agencies that have critical infrastructure responsibilities and industry sector coordinating mechanisms. Specifically, the Council is charged with:

- Enhancing cooperation between the public and private sectors in protecting information systems supporting critical infrastructures in key economic sectors and providing reports on the issue to the President, as appropriate;
- Enhancing cooperation between the public and private sectors in protecting critical infrastructure assets in other key economic sectors and providing reports on these issues to the President, as appropriate; and

- Proposing and developing ways to encourage private industry to perform periodic risk assessments of critical information and telecommunications systems.

The Council is composed of a maximum of 30 members, appointed by the President. The members of the NIAC are selected from the private sector, generally chief executive officers or their equivalent, including industry and academia, as well as public sector employees representing State and local governments. The members of the NIAC have expertise relevant to the functions of the NIAC with responsibilities for the security and resilience of critical infrastructure supporting key sectors of the economy, including agriculture, banking and finance, chemical, commercial facilities, critical manufacturing, dams, defense industrial base, government facilities, nuclear, postal and shipping, public health, transportation, information technology, communications, national monuments, energy, emergency services, and water.

Each year the NIAC undertakes several major studies in support of its mission. These studies focus on key topics selected by the NIAC to inform the President on emerging issues, developments, and trends related to infrastructure protection and resilience. Its reports have drawn public and private sector interest with regular requests from Congressional committees for copies. The NIAC meets publicly four times a year, hosted in Washington, D.C., in a venue open to the public.

Appendix B Selected Resilience Practices in the Electricity Sector

Note: U = Unintentional Acts I = Intentional Acts C = Cyber Acts A = Applies to All Acts

Robustness	
People and Processes	**Infrastructure and Assets**
• Execute announced and unannounced emergency drills for control centers (A) • Isolate control systems from IT systems and Internet (I, C) • Assist smaller utilities in increasing their resilience (A) • Place ISACs and other monitoring organizations on constant alert, ensuring quick emergency response(A) • Increase inventory of key components such as EHV transformers and protective relays (A) • Continuously expand understanding of emerging threats and adjustments to new threat environment (I) • Improve risk management plans in face of malicious acts such as terrorism (I) • Update risk management plans to reflect current risk forecasts (A) • Build muscular memory into exercises (A) • Hold tabletop exercises to determine what is on hand and what needs to be acquired; work with supply chain to ensure supplies will be available if needed (A) • Use Power System Simulation for Engineers model to build case studies 10–15 years out for resource planning and expected threats with annual increments (A) • Drill Emergency Response Plan at least once a year (A) • Provide Board of Directors with operational risk briefings (A) • Utilize proprietary fiber optic communications to ensure control of system (A) • Assign specific resources to resilience planning and implement improvements when it makes business sense to do so (A) • Conduct hurricane/disaster preparedness and training (U) • Comply with inspection protocols (A) • Develop plans to deal with N-2 attacks and multiple N-1 attacks (A) • Gain State and local government support in utility upgrades (A) • Expand cross-sector, cross-discipline, and cross-jurisdiction analysis of major incident impact on aging infrastructure and resulting cascading effects (A) • Establish risk management committee (A) • Continue to prove systems and components to find weaknesses and resolve them (A) • Cooperate closely with FBI to identify threats to transmission towers and other assets (I) • Work within partnerships to better understand threat and reconfigure control systems to avoid identified threat or incorporate protective measures (I, C) • Incorporate patches as required to improve cyber security (C) • Connect with HSIN and/or InfraGard for alerts and situational awareness (A) • Work with government on advanced projects such as responding to EMP events, which industry cannot handle on its own (A)	• Construct backup control center (A) • Build double-redundant transmission sections to handle N-2 failures (A) • Build transmission to fit customer needs (e.g., military) (A) • Use threat vectors, potential consequences, and cost-benefit analysis tools to determine best investments for additional system reliability and robustness while meeting standards (A) • Build resilience into a system based on analysis of contingencies: measures are cost-effective based on predictability of risk (A) • Develop standards that fit cyber threat but do not limit company's own cyber security efforts (C) • Build transmission to fit customer needs (e.g., military)—extra transmission lines to high-demand customers (A) • Plan resilience at two levels: the edge (end users) and core (deep within bulk electric power system) (A) • Design system (1) to prevent cascading failure (keep problems to self, while help and expect help from others as needed), and (2) to maintain continuity of service by moving electricity around as needed (A) • Build systems for high safety, high reliability, and low price – not guarantee of service (A) • Build under FERC rate base; go to local utilities commission to put line in (A) • Build transmission system for automatic transfer in case of single failure (N-1); some sections built for N-2 event (A) • Maintain backup analog system that can run if the digital control systems go out during a cyber attack (C) • Have two separate control centers operating off different lines; also two separate communications systems (A) • Build-in ability to fail gracefully: under-frequency relaying and SCADA systems designed to lose up to 30% of power in 10% incremental stages (A) • Maintain circuit overload protection (A) • Employ redundant power to nuclear plants for cooling systems (A) • Use firewalls to intercept hits from Internet (C) • Update aging equipment on regular basis (A) • Set relays so they are coordinated to prevent a cascading collapse of the local and neighboring grids (A) • Work with national labs to test control systems before becoming operational (C) • Build spare transformers into the system, but do not co-locate spare high-voltage transformers with those they are intended to replace (A) • Focus on designing system so that it is robust and can recover rapidly (A) • Deploy sensors and control technology (A) • Install asset databases/tools (A) • Manage vegetation (U) • Enhance IT and communications (A) • Design systems to fit specific geographic area and natural risks associated with that area (U)

Resourcefulness	
People and Processes	**Infrastructure and Assets**
• Monitor transmission in real time using "state estimators" (A) • Increase number of key employees with clearances (I) • Build info-sharing partnerships with key government agencies to obtain actionable open-source or FOUO info, as well as classified briefings if possible (I, C) • Cooperate with telecom to help resolve cyber issues (C) • Develop and utilize media communications plan to ensure accuracy in reporting (A) • Put plans in place to care for families of critical employees during emergencies (A) • Look at variety of contingencies in local area to ensure that higher value customers receive power even during hurricanes (A) • Have adequate replacement equipment in storage and rapidly deployable repair crews on standby (A) • Utilize detailed cooperative agreements within local and regional jurisdictions or with mutual assistance groups and draw upon staff drills (A) • Communicate appropriate emergency contact at jurisdictional meetings (A) • Maintain 24/7 Ops Center with focus on system integrity – operators must be hands-on, well-trained, and have automated system for shutdown to prevent cascading effect (A) • Use helicopters and air boats to get crews to downed lines when roads are blocked (A) • Utilize pre-arrangements with supply chain for access to key contract personnel and emergency products such as 4-wheel vehicles, big equipment, emergency fuel, emergency kits of equipment and supplies (A) • Have secure communications, including internal radio capabilities, portable cellular systems, a private communication network and/or satellite phones for back-up communication between control centers and substations (A) • Pre-deploy resources toward specific areas and work closely with suppliers in days before a storm (2-3 days) (A) • Activate the Vulnerability Response Team in an emergency; team can activate Emergency Response Plan if need be (A) • Keep list of recent retirees with current contact numbers in case need to temporarily contract them for assistance in repairs (A) • Improve employee communications and tracking (A) • Coordinate priority restoration and waivers (A) • Ensure that facilities are able to withstand another event within 30 minutes of the first (A) • Employ old telemetry (analog and not digital) to allow transmission to run, for a while, when SCADA or digital control systems are lost (C) • Create a storm readiness checklist (U) • Strengthen communications loops with DOD and FEMA • Ensure clear chain of command/lines of authority for decision making • Monitor system continuously with live operators (A) • Use local generation to enable additional capability in emergency (A)	• Automate system transfer for N-1 failure (A) • Build-in automatic shut down on grid to prevent cascading failure (A) • Maintain log of key equipment such as transformers on age, components, maintenance schedule, etc. (A) • Utilize Phasor technology to rapidly pick up problems on the grid (A) • Purchase or lease mobile transformers and substations (A) • Procure spare T&D equipment (A) • Install redundant communications (A) • Implement double dead-end structures to limit cascading events • Balance power needs of two major customers: customer base and special customers (critical nodes, defense, financial markets, energy refineries, possible targets) (A) • Employ two separate alert stages for failure: emergency (30 minutes before fail) and load shell limit (operator must act immediately) (A)

Rapid Recovery	
People and Processes	**Infrastructure and Assets**
• Enact mutual aid agreements for equipment and repair workers (A) • Develop a list of priority recovery electricity services with customers (e.g., hospitals, fire, police, emergency) (A) • Build system to allow rapid re-routing around problem, so that outages can be restored quickly (A) • Develop recovery plans with priorities – e.g., restore power to natural gas pipelines for combustible back-up systems, next restore communications, next restore Internet-based IT systems (A) • Cooperate with industry members on logistics, prepositioning, just-in-time training, and local procurement of supplies (A) • Utilize pre-arrangements with vendors to ensure continuity of supplies, or to identify alternate sources of supplies in case primary source is incapacitated (A) • Maintain black start capability (but practice on tabletop exercises because of danger of shutting down system). Restart nuclear plants first and reinstate stable transmission grid before restoring service (A) • Ensure rapid recovery by design – most systems under N-1, but many have double contingencies, and a few urban areas have triple contingencies (A) • Maintain rapid responders close to potential problems for quick recovery of specific line or system repairs (A) • Maintain fleet of mobile transformers (A) • Maintain inventory of spares at all times and increase if expect problem; also have contractual agreements with suppliers (including foreign suppliers) and identify alternatives in event of emergency needs (A) • Have elaborate system in place for service recovery: call centers; system-wide storm center; reallocation of resources to regions needing repairs; trucks loaded GPS systems; software to detail exactly what equipment is needed where and prepare that inventory for pick up by the trucks; supervisors can monitor work crews (A) • Restore system to appropriate stability and level of operability before try to connect with others during an emergency (A) • Facilitate employee evacuation and reentry (A) • Create safe warehousing provisions for hard-to-replace components, potentially government sponsored (A) • Maintain communication with CEOs of other utilities to let others "jump in line" for critical components with long lead times (A)	• Maintain shared inventory of spare EHV transformers, based on EEI CEO recommendations and agreement – prepared for 10 substation event (Spare Transformer Equipment Program – STEP) (A) • Maintain key assets in transmission: transformers; station/relay systems (can take weeks to bring back up, with no redundancy for these); large and small circuit breakers (A) • Have spare Lindsay towers on hands that can be put together to replace blown-down transmission towers (A) • Gain access to natural gas for generators (A) • Ensure easy movement of assets (highway infrastructure improvements or debris clearing) • Update general quality of black start generating units • Warehouse materials for electricity recovery – Tri-State example – important part of reliability and recovery (A) • Maintain ability to clear local roads when local communities do not clear them for the utilities to repair their infrastructure(A) • Develop and build a recovery transformer (A)

Adaptability	
People and Processes	**Infrastructure and Assets**
• Revised emergency response plan after lessons learned (e.g., from hurricanes, tornadoes, floods, other incidents) to include all hazards and be scalable (A) • Implemented NERC standards to continuously improve resilience (A) • Improved NERC reliability coordinator response to emerging cyber threat (C) • Included new vulnerabilities and interdependencies in planning scenarios for system improvement (A) • Continuously improve understanding of threat to systems (I) • Improved risk management for new emergency threats (I) • Made security part of planning process (A) • Always question what more needs to be done to address new order threats (A) • Reduced dependency on the Internet and limited access to SCADA/EMS systems (A) • Developed new risk processes for cascading failures (A) • Developed new risk processes for supply chains, as well as getting people to the plant and critical areas (A) • Founded North American Transmission Forum (NATF) after 2003 Blackout to improve transmission industry communication and cooperation through confidential phone calls (A) • Conducted annual exercises on generation and transmission to decide what to start first and what to start next (A) • Assigned employee to take notes during crisis so that after-action reports and analysis can be conducted and possible improvements identified for further analysis (A) • Have a secure control room, institute background checks for employees, and put into place tighter procedures for access to control systems and other facilities (A) • Instituted arrangements with local water utility to ensure that two lines instead of one goes to facility to cool equipment (A) • Continuously adding new contingencies to state estimator (A) • Continuously participating in tabletop exercises to know how to respond to various scenarios, determine roles and responsibilities, and improve resilience (A) • For cyber threats, trained operators to focus on two different scenarios: what is different from normal, and what is wrong. Must first understand what is happening (C) • Used “heat map” to identify consensus on areas of risk in order to focus resources (A) • Used committees to examine company risks and risk management: determine who is responsible for what (A) • Hold generation, transmission, and board-level-specific lessons learned sessions following incidents/exercises (A) • Looked at systemic risk rather than only asset risk (A) • Planned to isolate and bring back facilities, preventing cascading events like 2003 Blackout (A) • Learned resilience best practices from international partners such as Canada, Australia, and UK (A) • Updated strategic roadmap for industry (A) • Instituted more active engagement between Electricity SCC and industry (A) • Tried to plan for events larger than any yet experienced (A) • Began planning system 20 years in advance to foresee challenges such as incorporating renewables – took a holistic view on the evolution of the system (A)	• De-rated underground power line based on failure in another country (A) • Reconfigured lines based on known threats or vulnerabilities (I) • Tried to improve all systems and infrastructure or design new systems during investment and construction planning (A) • Encouraged R&D to mitigate identified vulnerabilities (e.g., modular EHV transformers and more manufacturers of protective relays) (A) • Moved power lines and transmission towers to other side of mountain away from river (U) • NERC worked on new designs to counter cyber and malicious attacks (I,C) • Based planning analysis on future threats (A) • Working on adjusting national policy to provide justification for hardening system against EMPs (A) • Focused more on low-probability, high-consequence events – however, planning and implementation is very expensive so need good information on which to base decision (A) • Industry tried to improve resilience incrementally rather than all at once -- hard to do major improvement in protection and resilience unless compelling demand from government or public – too expensive and takes a long time to replace equipment (A) • Moved planning scenarios from 400,000 customers losing power to nearly 800,000 during Hurricane Floyd (U) • Began working with government to utilize their help in several ways: expedite mutual assistance; ensuring fair system of utility costs; help in moving assets during an emergency; provide safe warehousing for hard-to-replace equipment such as high voltage transformers; encourage domestic production of key equipment; share more information about cyber threats; what to look for in potentially harmful employees; cross-sector and interdependencies analysis; analysis of impact of aging infrastructure and possible cascading events (A) • Replaced straight high-voltage transmission towers with double dead-end (storm structures) so entire line won’t collapse in ice storm (A) • Began keeping larger inventory of needed replacements (A) • Based on study results, began doubling control center capability so that any 500kV substation can be used as a control center for the entire system (A) • Developed better battery capabilities and supplies • Encouraged domestic production of transformers that will not be subject to potential trade disputes • When possible, used updated parts rather than old ones when repairing facility or system (A) • Elevated substations/control rooms/pump stations on stilts, etc. following unpredicted floods(U) • Relocated/constructed new lines and facilities (A) • Upgraded damaged poles and structures (A) • Strengthened poles with guy wires (A) • Buried power lines underground (A)

Adaptability	
People and Processes	**Infrastructure and Assets**
• Evaluated risk conditions differently, based on geographic vulnerabilities • Limited information on the Internet about substations and other essential grid components • Continue cooperation with local and regional law enforcement and improve coordination with Federal law enforcement for imminent threats on the national scale • Examining common standards for high-voltage transformers	

Appendix C Nuclear Sector Case Study

The nuclear reactors, materials, and waste sector (nuclear sector) is one of 18 Critical Infrastructure and Key Resources (CIKR) sectors defined by the Homeland Security Presidential Directive 7 (HSPD-7) and includes several elements:

- Nuclear power plants
- Research, training, and test reactors
- Deactivated nuclear facilities
- Fuel cycle facilities
- Nuclear materials transport
- Radioactive materials
- Radioactive source production and distribution facilities
- Nuclear waste

Not included in the nuclear sector are Department of Defense (DoD) and Department of Energy (DOE) nuclear facilities or radioactive material associated with defense activities. This case study will focus on nuclear power plants, with some reference to the other elements within the sector.

Nuclear energy provides about 20 percent of the electricity in the United States through 104 reactors in 65 nuclear power plants located in 31 States dispersed across the Nation. In the United States there are 32 companies licensed to operate nuclear reactors (referred to as licensees). In 2009, nuclear power plants in the United States generated electricity equivalent to nearly 800 billion kilowatt-hours. Except when down for maintenance or refueling, most reactors function at more than 90 percent capacity. Once fueled, nuclear reactors can operate continuously for about two years.[18]

Critical Interdependencies

The nuclear sector has several interdependencies. The most important of these is the electricity sector. Large power plants generally have no electricity power storage capability; therefore, the electricity generated by the plants must immediately be channeled through the transmission lines of the electricity sector. If all transmission lines to a nuclear power plant are down, then the plant must go to cold shutdown for safety purposes. On the other hand, the electricity sector in many regions of the country depends on the nuclear sector for a reliable source of electricity to stabilize the grid and enable the efficient distribution of the load.

The healthcare and public health sector is highly dependent on the nuclear sector for nuclear and radiological facilities and materials. Conversely, the radioisotopes community is dependent on the transportation and shipping sectors to get the materials to the healthcare sector. Other nuclear sector interdependencies include emergency services; information technology (IT), which controls critical processes; telecommunications, which services much of the industry's communications; and chemical, which produces substances used at fuel cycle facilities.

[18] Nuclear Energy Institute, "U.S. Nuclear Power Plants: General Statistical Information."

Infrastructure Design and Regulation

Because of the radiological materials used and produced by the nuclear sector, the consequences of a nuclear facility being damaged or destroyed through any event—unintentional (accident or natural disaster), intentional (terrorist or insider threat), or cyber (unauthorized intrusion into control systems)—could threaten public health and safety or the environment.

These potential consequences have been recognized from the inception of the Nation's nuclear power program. Both industry and government have made extraordinary efforts to protect the public and the environment from a radiological release. As a result, the nuclear sector is one of the most regulated of the CIKR sectors; its risk analysis and risk management practices are highly developed, and its facilities are very robust and hardened.

The Atomic Energy Act was passed in 1957, and the Atomic Energy Commission regulated all aspects of the nuclear industry from the very early days. The U.S. Nuclear Regulatory Commission (NRC) was created as an independent agency by Congress in 1974 to enable the nation to safely use radioactive materials for beneficial civilian purposes while ensuring that people and the environment are protected. The NRC regulates commercial nuclear power plants and other uses of nuclear materials, such as nuclear medicine, waste, and the entire fuel cycle, through licensing, inspection and enforcement of its requirements.

The Nuclear Energy Institute (NEI) is the U.S. trade association and policy institute representing the nuclear energy industry and serving as its single point of contact. It purpose is to support the nuclear energy industry by providing policy direction on critical issues; presenting a unified industry approach to regulatory and policy issues; representing the industry before Congress, executive branch agencies, regulatory bodies, State policy forums, the media, and the general public; and assisting the nuclear energy industry with regard to State issues such as environmental considerations and rates. Other industry organizations with overlapping interests in the sector include the Electric Power Research Institute and the American Nuclear Society.

NEI serves as the implementing organization for key nuclear sector stakeholders who make up the members of the Nuclear Sector Coordinating Council (NSCC). The counterpart to NSCC is the Nuclear Government Coordinating Council (NGCC), which includes the Department of Homeland Security as the Chair, the Nuclear Regulatory Commission, Department of Energy, Department of Transportation, Federal Bureau of Investigation, State regulators, Federal Emergency Management Agency, and other offices within DHS such as the U.S. Coast Guard and Domestic Nuclear Detection Office.

Nuclear power plants are exhaustively engineered and designed to withstand almost all conceivable manmade and natural hazards, short of an act of war (see Exhibit C.1). Protection and resilience are built into the design and operation of the facility. Additional layers of protection and resilience are added when credible new threats are identified.

Exhibit C.1 Hurricane Ike, September 2008

Hurricane Ike was the third costliest hurricane ever to strike the United States. At times a Category 4 hurricane, Ike made its final landfall near Galveston, Texas, as a strong Category 2 hurricane, with Category 5 equivalent storm surge, on September 13, 2008. Hurricane-force winds extended 120 miles from the center. The storm resulted in the largest evacuation in Texas's history.

The South Texas Project (STP) nuclear plant, located near Bay City about 80 miles southwest of Houston, generates more than 7 percent of the electricity used in Texas. STP took precautionary steps at its two reactors to go offline if winds from Hurricane Ike exceeded 70 mph, but winds of 65 mph were experienced at the facility and the twin-reactors stayed online.

Nonetheless, the hurricane knocked down transmission lines and several non-nuclear power plants were shut down. There was risk of blackouts. The STP nuclear plant has about 4 different transmission hubs that it can connect to. Three of the southern and eastern line systems were down. The one to the west held up. Because of this transmission connection, the plant managed to operate through the weather emergency and keep the lights on, when other components of the electricity sector were failing.

STP Reactor Containment Buildings
Size: 200 feet above ground, 41.5 feet underground, 150 feet wide
Outer Wall: Steel-reinforced concrete, four feet thick
Lining: Fully lined with 3/8-inch-thick, carbon steel plates
Inner Walls: Steel-reinforced concrete, totaling eleven feet thick
Foundation: Concrete, 18 feet thick
Houses: Reactor, pressurizer, steam generators, reactor coolant pumps, associated piping and tubing, and support systems.
Item: More than 500,000 cubic yards of concrete and 119 million pounds of steel reinforcing bars are in STP's two reactor containment buildings. The structures can withstand a Category 5 hurricane, a 1.9G earthquake and the impact of a Boeing 767 fully loaded with fuel.

Source: South Texas Project Nuclear Power Plant, "STP Nuclear Power Plant: Facts and Stats."

Understanding and minimizing the risks of nuclear proliferation and terrorism is one of the four central objectives of DOE's Office of Nuclear Energy (DOE-NE), as laid out in the *Nuclear Energy Research and Development Roadmap: Report to Congress*, published in April 2010. DOE is concerned with government entities diverting nuclear technology illicitly in pursuit of weapons (proliferation resistance) and terrorists obtaining materials for a nuclear device (physical protection). While the former is primarily of interest in the international arena, the latter impacts the domestic nuclear industry as well. DOE's research program to strengthen proliferation and security defenses includes more robust risk assessment methods, improved instrumentation and controls, and high-performance modeling and simulation. These efforts are consistent with a second Roadmap objective to improve the reliability, sustain safety, and extend the life of the current reactor fleet. DOE has already established a Modeling and Simulation Hub at Oak Ridge National Laboratory to provide a state-of-the-art multi-physics computational environment for nuclear analysis.

DOE-NE has also requested funding in FY 2011 to initiate the Nuclear Energy Enabling Technologies (NEET) Program, which seeks to overcome obstacles to expanded nuclear energy use. An inaugural workshop to kick off this new program was held July 29, 2010. Integral to the program mission is development of new instrumentation and control technologies that address new cyber security needs; provide resilient controls; improve monitoring, diagnostic, and prognostic capabilities; and enhance the communications that enable these technologies to work together. Of equal importance to the NEET mission is ensuring that nuclear systems are robust and proliferation-resistant; robustness includes preventing the sabotage of nuclear facilities or transportation. Program efforts will lead to innovative tools and methodologies for assessing, comparing, and managing the proliferation and terrorism risks of nuclear energy technology and fuel cycle systems.

The nuclear sector emphasizes defense in depth, redundancy, and mitigation analysis. The emphasis is on physical security, and the most critical assets are the nuclear reactor and its protected areas, and the radioactive material that it contains. In addition to physical security, emergency preparedness is critical to the nuclear sector. The NRC has extensive regulations that industry must follow in regards to both physical security and emergency preparedness.

The nuclear power industry has decades of experience in physical security and emergency preparedness. Security procedures are exceedingly robust, layered, and exercised. Security officers are trained and armed, and have the right to use deadly force in accordance with Federal and State laws. Examples of these security and preparedness practices can be found throughout this case study.

The nuclear sector is proactive in improving the security of its nuclear power plants and other sector elements. This includes participation in the DHS Comprehensive Review (CR) process and the tracking of voluntary enhancements to power plant security through the Comprehensive Review Outcomes Working Network (CROWN). All U.S. organizations that operate commercial nuclear power plants are members of the Institute of Nuclear Power Operations (INPO), established in 1979 to help the nuclear power industry achieve the highest levels of safety and reliability (see Exhibit C.2).

Improvement in industry security is further facilitated through an active program of lessons learned in which NEI members of the Nuclear Strategic Issues Advisory Committee (NSIAC) consider enhancements to security and vote on which to implement industry wide.

Exhibit C.2 Institute of Nuclear Power Operations (INPO)

INPO was created by the nuclear power industry in response to a recommendation from the Kemeny Commission, set up by President Jimmy Carter to investigate the March 1979 accident at the Three Mile Island nuclear power plant. Funded and supported by the U.S. nuclear industry, INPO is intended to promote operational excellence and improve the sharing of operational experience between nuclear power plants.

The primary work of INPO revolves around four key activities:

- Nuclear power plant evaluations held on a regular basis
- Training through the National Academy for Nuclear Training and accreditation using established performance objectives, criteria, and guidelines for the nuclear power industry
- Review and analysis of any significant event at nuclear electric generating plants, and communication of lessons learned and best practices throughout the nuclear power industry through information exchange and publications
- Assistance to help plants continually improve their performance, specifically providing assistance on technical or management issues at the request of individual nuclear electric generating facilities.

Source: INPO, “About Us.”

The Nuclear Sector Risk Profile

There are two general categories of risk in the nuclear sector: risks to nuclear and radiological facilities, and risks to nuclear and radiological materials.[19] Risks to facilities, including nuclear power plants, include such things as natural disasters, accidents, terrorist attack, and sabotage from within the facilities themselves. In recent years, cyber security has emerged as another risk factor to facilities, in that control and other vital systems essential to the safe and secure functioning of the facility might be compromised through cyber attack.

Risks to nuclear and radiological materials include theft and diversion from its intended use. Also of concern is the possibility of supply chain disruption, including interruption to the proper end-of-life disposal of nuclear and radiological waste.

Nuclear power plants supply about 20 percent of the Nation's power, and there are more than 100 reactors around the country. If one or more reactors should be shut down for any reason, the electric grid itself would not be damaged. Of greater concern from a risk perspective is the unauthorized access to, use, or release of nuclear and radiological material. Release of radioactive materials at the level of those found in nuclear facilities can cause significant loss of life, economic disruption, and social-psychological impact. In addition, of particular concern in the post 9/11 era is the use of nuclear or radiological material in an improvised nuclear device (IND) or radiological dispersal device (RDD).

The nuclear sector is designed and operated to mitigate these risks and to rapidly respond to and recover from any incident that may occur.

Resilience in the Nuclear Sector

The nuclear industry does not routinely use the term "resilience." The common terms describing resilience-related practices are robustness, reliability, and defense in depth. As required by the 2009 National Infrastructure Protection Plan (NIPP), however, resilience is increasingly being considered along with protection as part the NIPP Risk Management Framework, which all CIKR sectors must address in their Sector Specific Plans (SSPs) and Sector Annual Reports (SARs).

Nuclear sector practices related to robustness, reliability, and defense in depth, coupled with emphasis on emergency preparedness and the industry process of adopting lessons learned through ongoing operating experience, exhibit all of the elements of the NIAC resilience construct (described in Section 2): robustness, resourcefulness, rapid recovery, and adaptability.

Robustness: Nuclear Power Plant Security

NRC holds nuclear power plants to the highest security standards of any American industry. Security regulations are based on a "design basis threat," which is characterized as a suicidal, well-trained paramilitary force, armed with automatic weapons and explosives, and intent on forcing its way into a nuclear power plant to commit radiological sabotage. The design basis threat is reviewed annually and updated as new intelligence and law enforcement information comes into the NRC.

[19] U.S. Nuclear Regulatory Commission, "Frequently Asked Questions About NRC's Design Basis Threat Final Rule."

Although details are not publicly available, plant security is multi-layered and includes physical security, cyber security, and personnel security. The same stringent security measures in place to protect nuclear power plant reactors are applied to the storage of used nuclear fuel at the site.[20]

Physical security starts with the infrastructure of the facility itself. Each plant is designed for reliability of plant systems, redundancy, and diversity of key safety systems. Nuclear plant security zones include the owner controlled area, protected area, and vital area—each with more robust layers of access control and protection. The reactors themselves are steel-reinforced concrete structures constructed to withstand earthquakes, hurricanes, tornadoes, and floods. Exhaustive analysis by NRC determined that an airplane attack on a nuclear power plant would be unlikely to affect public health and safety, and the Electric Power Research Institute confirmed that the primary structures of a nuclear plant would withstand the impact of a wide-body commercial airliner.[21]

Additional physical security measures include extended and fortified security perimeters, barriers and illuminated detection zones, well-trained and well-equipped armed security officers on duty 24/7, surveillance and patrols, intrusion detection devices such as high-tech surveillance equipment, bullet-resistant barriers to critical areas, vehicle and personal search, barriers to protect against vehicle bombs, multiple access control points, a dedicated contingency response force, and force-on-force training exercises to evaluate security officer response to mock adversary attacks. There is also close coordination of site security forces with external law enforcement responders.

Cyber security measures include isolation of control system computers from the Internet; the industry-wide implementation of cyber security guidelines developed in cooperation with the Pacific Northwest National Laboratory; NRC approval of plant cyber security plans to ensure the capability for timely detection and response to cyber attacks; mitigation of the consequences of such attacks; the correction of exploited vulnerabilities, and restoration of affected systems, networks, and equipment; and ongoing assessments of cyber security including quarterly briefs by DHS on new cyber security threats.

Personnel security measures include enhanced psychological assessments, fingerprinting, and background checks for employees; information sharing on personnel between reactor licensees; access controls; insider threat mitigation programs; repeated drills and testing of security response and emergency procedures, including keeping the plant safe from attempted sabotage; and biometric and other identification to enter sensitive areas.

Resourcefulness and Rapid Recovery: Emergency Preparedness for Nuclear Power Plants

The nuclear power industry has over four decades of operating experience. Over the years, its emergency preparedness plans have been subject to evolving regulation and guidance from NRC and FEMA, as well as through many agencies at Federal, State, and local government levels.[22] The purpose of nuclear power plant emergency preparedness regulations is to ensure that the public is protected in the event of an accident at a nuclear power plant. Regulations facilitate standardization of emergency preparedness across the industry, including the integration of nuclear power plant licensee, offsite response organization, and Federal emergency plans and programs. There is close interface between all

[20] Nuclear Energy Institute, "Key Issues: Plant Security."
[21] U.S. Nuclear Regulatory Commission, "Security Spotlight."; Electric Power Research Institute, "Deterring Terrorism: Aircraft Crash Impact Analyses Demonstrate Nuclear Power Plant's Structural Strength."
[22] See, for example, U.S. Department of Homeland Security Federal Emergency Management Agency, *National Response Framework: Nuclear/Radiological Incident Annex*.

stakeholders in emergency preparedness to protect public health and safety from an accident at a nuclear power plant.[23]

Among the regulations governing nuclear power plant emergency preparedness are 16 planning standards (or capabilities), two emergency planning zones (10-mile plume exposure pathway and 50-mile ingestion exposure pathway), and annual letters of certification for State and local plans. The 16 planning standards are established by NRC and FEMA and include such capabilities as on-site emergency response organizations, notification methods, emergency communications, accident assessment, protective response, radiological exposure control, recovery and reentry, and exercises and drills.

In addition, the industry adheres to a standardized, four-level emergency classification system, ranging from notification of unusual events to general emergency. Both on-site and offsite response plans contain detailed guidelines for each emergency classification level.

Notification procedures also are regulated, with detailed plans agreed to and practiced by all stakeholders, including State and local emergency response agencies. There are secure communications dedicated to emergency notification, and these have backup systems in place. All notification procedures are routinely exercised.

Training, drills, and evaluated exercises are an important part of the sector's emergency preparedness. On-site staff are required to be trained and requalified annually, and emergency drills are held quarterly. Offsite response organizations also have annual training programs and certification, as well as drills and exercises. Biennially, there are integrated exercises which involve all response agencies with a 10-mile emergency planning zone. These exercises are evaluated by NRC and FEMA and include demonstrations of all major planning elements. The results are presented in a public hearing and published report.

Since the September 11th attacks, law enforcement has been added as a stakeholder in nuclear power plant emergency preparedness. Also, the preparedness framework has been brought into alignment with the Incident Command System (ICS) of the National Incident Management System (NIMS).

Adaptability: Nuclear Sector Comprehensive Review Process

All 104 of the Nation's nuclear power reactors voluntarily participated in DHS Comprehensive Reviews between 2005 and 2007. The CR process and its use by the nuclear sector to identify potential enhancements to sector protection and resilience are described below.

Comprehensive Reviews

The DHS Office of Infrastructure Protection (IP) uses the Comprehensive Review process to identify security enhancements and protective measures of an identified CIKR facility.[24] This voluntary program involves close coordination between IP's Protective Security Coordination Division, the facility's private sector owners and operators, State and local homeland security officials, and several core Federal team members including IP's Sector-Specific Agency Executive Management Office, the U.S. Coast Guard, the FBI, NRC, Transportation Security Agency, and FEMA. In the case of the nuclear sector CRs, other participants included the Environmental Protection Agency and the National Cyber Security Division; State Homeland Security Advisors; other State, county, and local emergency managers and planners;

[23] Nuclear Energy Institute, "Fact Sheet: Emergency Preparedness Near Nuclear Power Plants;" Nuclear Energy Institute, "Emergency Preparedness for Nuclear Power Plants," Draft PowerPoint Presentation, July 22, 2010.
[24] U.S. Department of Homeland Security, "Comprehensive Reviews."

emergency response agencies; representatives from the Nuclear Sector Coordinating Council; and various private representatives and associations (including NEI).

The CR process is a series of steps for planning, execution, and analysis of response to events beyond the regulatory basis. Of primary importance is the consideration of potential terrorist actions, the consequences of such an attack, and the integrated preparedness and response capabilities of the facility's owners and operators, local law enforcement, and emergency response organizations. Among the scenarios considered are ground, maritime, or aerial assault; bombings; vehicle-borne improvised explosive devices; nuclear, radiological, biological, or chemical material used as a weapon; and cyber attack.

Analysis is used to determine potential enhancements between existing regulated security and emergency response capabilities and additional capabilities that could be considered to prevent, defend, mitigate, and respond to terrorist threats, attacks, or scenarios such as those listed above, beyond design basis threats. This analysis results in the identification of potential enhancements, such as additional security or response capabilities, that could reduce the facility's and adjacent community's vulnerability in the event of a terrorist attack or all-hazards event. Compiled in a comprehensive Integrated Protective Measures Analysis (IPMA), this information can be used by stakeholders to inform future investment decisions or point to areas where additional research is required.

Nuclear Sector CRs and CROWN

The NEI executive-level Nuclear Strategic Issues Advisory Committee determined that it would be in the interests of the industry to have all of its reactors take part in the Comprehensive Review process. As mentioned, participation in the CRs is voluntary and, in the case of the nuclear sector, all identified enhancements to facility protection and resilience are above and beyond the stringent security standards already in place through NRC and other sector regulatory agencies. Therefore, most identified potential enhancements were "outside the fence" of the nuclear power plant facility and involved State and local law enforcement and emergency response stakeholders, as well as Federal elements such as the FBI and the U.S. Coast Guard.[25]

An enhancement is defined as the difference between existing security and emergency response capabilities and the additional capabilities that may enhance the preparedness or response with regard to terrorist-initiated actions. For each identified enhancement, a specific option to be considered for implementation is provided in the Integrated Protective Measures Analysis report for each site.

The CRs followed a nuclear power plant risk analysis and management for critical asset protection (NPP RAMCAP) methodology developed for the sector by the Electric Power Research Institute in coordination with DHS. A description of the methodology can be found in EPRI Technical Report 1011767 dated December 2005.[26] The NPP RAMCAP methodology involves a series of steps—asset characterization, threat characterization, consequence analysis, vulnerability analysis, threat assessment, risk assessment, and risk management—applied to critical plant facilities subject to benchmark threats such as attack by aircraft, vehicle- and water-borne improvised explosive devices, and armed attack from trained personnel. The final step in the process—risk management—results in the identification of risk goals and recommendations, and the evaluation of options and decisions on security enhancements.

[25] U.S. Department of Homeland Security, "Nuclear Sector Comprehensive Reviews."
[26] Electric Power Research Institute, "Nuclear Power Plant Risk Analysis and Management for Critical Asset Protection (RAMCAP) Trial Applications Summary Report."

To follow up on suggested enhancements identified in the CR process, the nuclear sector established a Comprehensive Review Outcomes Working Network, comprising agencies involved with the CRs. CROWN analyzed the extent to which the enhancements were addressed by State and local law enforcement and emergency management organizations, industry, and the Federal government. To do its work, CROWN reached out to all sector stakeholders to facilitate the enhancements where feasible and appropriate, and provided grant and training information where appropriate. CROWN utilized the information from the IPMAs to create a "menu" of enhancements for stakeholders to consider as a basis for risk-informed investments and R&D decisions.

To facilitate implementation, CROWN divided responsibility for the enhancements into four points of contact: the FBI for tactical teams and site take-back; the U.S. Coast Guard (USCG) for areas under their responsibility, such as maritime issues; NEI for "inside the fence" enhancements; and the SSA EMO for remaining enhancements, including emergency preparedness, bombing, non-USCG related maritime issues, and buffer zones. CROWN further established a tracking mechanism for enhancement implementation based on four criteria: implemented, in process of implementation, planned to be implemented, and not necessary to implement.

The CROWN project ended at the close of 2009. Of the several hundred enhancements considered worthy of implementation, roughly half have been fully implemented or are in the process of implementation. In the interests of security, the exact number of potential enhancements and their details have not been released to the public.

Sector Goals

The nuclear sector does not define its sector goals in terms of resilience, although sector goals can be mapped fairly closely to resilience. The NRC *Strategic Plan FY 2008–2013* lists two goals and several strategic outcomes for the sector:

Goal One: Safety—Ensure adequate protection of public health and safety and the environment.
Strategic Outcomes:

- Prevent the occurrence of any nuclear reactor accidents.
- Prevent the occurrence of any inadvertent criticality events.
- Prevent the occurrence of any acute radiation exposures resulting in fatalities.
- Prevent the occurrence of any releases of radioactive material that result in significant radiation exposures.
- Prevent the occurrence of any releases of radioactive materials that cause significant adverse environmental impacts.

Goal Two: Security—Ensure adequate protection in the secure use and management of radioactive materials.
Strategic Outcome:

- Prevent any instances where licensed radioactive materials are used domestically in a manner hostile to the United States.

By way of comparison, the Nuclear SCC and GCC agreed on eight security goals for the nuclear sector public-private partnership to pursue above and beyond existing regulation.[27] These goals—centered around the categories of awareness; prevention; and protection, response, and recovery—are:

Awareness

Goal 1: Establish permanent and robust collaboration and communication among all stakeholders having security and emergency response responsibilities for the nuclear sector.

Goal 2: Obtain information related to other CIKR assets' dependencies and interdependencies with the nuclear sector and share it with sector security partners.

Goal 3: Increase public awareness of sector protective measures, consequences, and proper actions following a release of radioactive material.

Prevention

Goal 4: Improve security, tracking, and detection of nuclear and radioactive material in order to prevent it from being used for malevolent purposes.

Goal 5: Coordinate with Federal, State, and local law enforcement agencies to develop protective measures and tactics to deter, detect, and prevent terrorist attacks on nuclear facilities and other nuclear sector assets.

Protection, Response, and Recovery

Goal 6: Protect against exploitation of the nuclear sector's cyber assets, systems, networks, and the functions they support.

Goal 7: Use a risk-informed approach that includes security considerations to make budgeting, funding, and grant decisions on all identified potential protection and emergency response enhancements.

Goal 8: Enhance the ability of Federal, State, territorial, local, and tribal governments, and the private sector to effectively respond to nuclear and radiological emergencies that result from terrorist attacks, natural disasters, or other incidents.

In terms of the resilience construct defined by the NIAC in this case study—robustness, resourcefulness, rapid recovery, and adaptability—the goals identified by NRC and by the Nuclear Sector SCC and GCC fall mostly within the robustness and resourcefulness dimensions, and all but one of the goals fall across more than one dimension. This is reflected in Exhibit C.3.

[27] U.S. Department of Homeland Security Office of Infrastructure Protection, Sector Specific Agency Executive Management Office, "National Infrastructure Protection Plan."

Exhibit C.3 Nuclear Sector Goals and NIAC Elements of Resilience

Nuclear Sector Goals	NIAC Elements of Resilience			
	Robustness Ability to absorb shocks and keep operating	Resourcefulness Managing a disaster as it unfolds	Rapid Recovery Getting back to normal as quickly as possible	Adaptability Absorbing new lessons from a catastrophe
NRC Goal 1	X	X	X	
NRC Goal 2	X	X		
SCC/GCC Goal 1	X	X	X	
SCC/GCC Goal 2		X		X
SCC/GCC Goal 3		X	X	
SCC/GCC Goal 4	X			
SCC/GCC Goal 5	X	X		X
SCC/GCC Goal 6	X			
SCC/GCC Goal 7	X	X	X	X
SCC/GCC Goal 8		X	X	X

Conclusions

Several conclusions can be drawn from this case study which may have relevance to CIKR sector resilience in general:

- **High regulation among a small number of owners and operators gives the nuclear sector strong resilience**. The nuclear sector is one of the most regulated of the CIKR, its risk analysis and risk management practices are highly developed, and its facilities are very robust and hardened. The NRC closely regulates commercial nuclear power plants and other uses of nuclear materials, such as nuclear medicine, waste, and the entire fuel cycle, through licensing, inspection and enforcement of its requirements.
- **Close relationship with the Federal government benefits the sector through security-related research and development**. The Department of Energy and its associated national laboratories maintain a vigorous program of activities related to security in the nuclear sector. These programs include research and development focused on advanced methods for manufacturing and construction, risk assessment methods, improved instrumentation and controls, and high-performance modeling and simulation.
- **The nuclear sector emphasizes physical security and rapid response, giving it strong "up-front" resilience practices**. In a sector where little to no failure is tolerated, its regulations and best practices are designed to mitigate sector risks and to rapidly respond to and recover from any incident that may occur. Most resilience practices in the nuclear sector are concentrated in the robustness and resourcefulness categories of resilience, rather than rapid recovery. This demonstrates the sector's "up front" approach to resilience, focused on nuclear power plant safety, security, and emergency preparedness.
- **Sector resilience can benefit from formal processes of gap analysis and structured enhancements from lessons learned.** The nuclear sector maintains a vigorous program of implementing lessons learned from previous incidents and extensive exercises and drills. The establishment of INPO has contributed significantly to industry improvement over the last 30 years through its various programs, including information exchange. The Comprehensive Review process has helped sector stakeholders identify enhanced security and preparedness measures beyond the already high level of security and preparedness required by law.

Appendix D References

"All-Hazards Planning: Core Business Priority Designations," *Edison Electric Institute Business Continuity Update* (2009): 2–4.

"Massive flooding hits Nashville," *Nashville Business Journal*, May 3, 2010. http://nashville.bizjournals.com/nashville/stories/2010/05/03/daily1.html.

Albert, Réka, István Albert, and Gary L. Nakurado. *Structural Vulnerability of the North American Power Grid.* January 7, 2004. http://arxiv.org/PS_cache/cond-mat/pdf/0401/0401084v1.pdf.

Anderson, Robert S., *Cyber Security and Resilient Systems*. Idaho Falls, ID: Idaho National Laboratory, July 2009. www.inl.gov/technicalpublications/Documents/4311316.pdf.

AT&T. *2010 AT&T Business Continuity Study: U.S. National Results*. Dallas: AT&T, 2010. www.att.com/Common/about_us/files/business_continuity/BusinessContinuity_2010_Summary.pdf.

Auerswald, Philip, and Debra van Opstal, "Coping with Turbulence: The Resilience Imperative," *Innovations: Special Edition for the World Economic Forum Annual Meeting 2009*, (2009): 203–218. Cambridge, MA: Davos-Klosters. www.compete.org/images/uploads/File/PDF%20Files/INNOVATIONS-Davos-2009_Auerswald-vanOpstal.pdf.

Australian Government. *Critical Infrastructure Resilience Strategy*. Barton, Australia: Australian Government, 2010. www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(9A5D88DBA63D32A661E6369859739356)~Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF/$file/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF.

Australian Government. *Critical Infrastructure Resilience Strategy Supplement: An overview of activities to deliver the Strategy*. Barton, Australia: Australian Government, 2010. www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(9A5D88DBA63D32A661E6369859739356)~Australian+Government+s+Critical+Infrastructure+Resilience+Strategy+Supplement.PDF/$file/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy+Supplement.PDF.

Baker, Scott, Shaun Waterman, and George Ivanov. *In the Crossfire: Critical Infrastructure in the Age of Cyber War – A global report on the threats facing key industries*. Santa Clara, CA: McAfee, Inc., 2010. http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf.

Baldor, Lolita C. "Computer hackers look to take over power US plants." Alpharetta, GA: SecurityInfoWatch.com. August 4, 2010. www.securityinfowatch.com/Utilities+%2526+Public+Works/1317096.

Bast, Gautam. "Supply Chain Risk Management: A Delicate Balancing Act." Somers, NY: IBM, 2008. ftp://ftp.software.ibm.com/common/ssi/rep_wh/n/GBW03015USEN/GBW03015USEN.PDF.

Behr, Peter. "Md.'s veto of advanced meter deployment stuns smart grid advocates." *The New York Times.* June 23, 2010. www.nytimes.com/cwire/2010/06/23/23climatewire-mds-veto-of-advanced-meter-deployment-stuns-95998.html.

Behr, Peter. "Regulators assess the ultimate blackout threat." *ClimateWire.* (July 2, 2010). www.eenews.net/public/climatewire/2010/07/02/1.

Behr, Peter. "Smart Meters." *ClimateWire.* June 25, 2010.

Borg, Scott. "Securing the Supply Chain for Electronic Equipment: A Strategy and Framework." Internet Security Alliance. www.whitehouse.gov/files/documents/cyber/ISA%20-%20Securing%20the%20Supply%20Chain%20for%20Electronic%20Equipment.pdf.

Briggs, Rachel, and Charlie Edwards. *The Business of Resilience: Corporate security for the 21st century*. London: Demos, 2006. www.demos.co.uk/files/thebusinessofresilience.pdf.

Brown, Theresa. "Dependency Indicators." *Wiley Handbook of Science and Technology for Homeland Security*, edited by John G. Voeller. Hoboken, NJ: Wiley, 2010. www.sandia.gov/nisac/docs/Dependency%20Indicators%20article%20w%20figs.doc.

Chang, Stephanie E. "Infrastructure Resilience to Disasters." *The Bridge* 39, 4 (2009): 36–41. Washington, D.C.: National Academy of Engineering. www.nae.edu/File.aspx?id=17673.

Council on Competitiveness. *Transform – The Resilient Economy: Integrating Competitiveness and Security*. Washington, D.C.: Council on Competitiveness, 2007. www.tisp.org/index.cfm?pk=download&id=11018&pid=10261.

CSIS Commission on Cybersecurity for the 44th Presidency. *Securing Cyberspace for the 44th Presidency*. Washington, D.C.: Center for Strategic and International Studies, December 2008. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Daly, Sue. "NARUC's Critical Infrastructure Efforts." Presented to National Association of Regulatory Utility Commissioners Summer 2006 Water Committee Meetings, San Francisco, July 31, 2006, www.narucmeetings.org/Presentations/water_daly_s06.pdf.

Edison Electric Institute. "EEI Principles for Cyber Security and Critical Infrastructure Protection." Washington, D.C.: Edison Electric Institute, September 9, 2010.

Electric Power Research Institute. *Deterring Terrorism: Aircraft Crash Impact Analyses Demonstrate Nuclear Power Plant's Structural Strength.* Palo Alto, CA: Electric Power Research Institute, December 2002. www.stpnoc.com/EPRI%20study.doc.

Electric Power Research Institute. *Nuclear Power Plant Risk Analysis and Management for Critical Asset Protection (RAMCAP) Trial: Applications Summary Report*. Palo Alto, CA: Electric Power Research Institute, December 2005. http://my.epri.com/portal/server.pt?Abstract_id=000000000001011767.

Emergency Management and Response Information Sharing and Analysis Center. "The Concept of Resiliency." *EMR-ISAC INFOGRAM 16-10*. Emmitsburg, MD: U.S. Fire Administration, April 22, 2010. www.usfa.dhs.gov/downloads/pdf/infograms/16_10.pdf.

Fedora, Philip A. "Reliability Review of North American Gas/Electric System Interdependency." Presented by the Northeast Power Coordinating Council. Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Track 2, 2004. www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2004.1265195.

Flynn, Stephen E. "America the Resilient: Defying Terrorism and Mitigating Natural Disasters." *Foreign Affairs.* Tampa, FL: Council on Foreign Relations, March/April 2008. www.foreignaffairs.com/articles/63214/stephen-e-flynn/america-the-resilient.

Flynn, Stephen E. "We're still not ready for another Hurricane Katrina." *Washington Post.* August 29, 2010: B2.

Florida Reliability Coordinating Council. *FRCC System Disturbance and Underfrequency Load Shedding Event Report*. FRCC Event Analysis Team, October 20, 2008.

Fujii, Andrea. "Pumping Station Repaired, Water Pumped Into System." *Channel 13 WJZ*. April 8, 2010. http://wjz.com/local/Northern.Baltimore.County.2.1616420.html.

Gas/Electricity Interdependency of the NERC Planning Committee Task Force. *Gas/Electricity Interdependencies and Recommendations.* Princeton, NJ: North American Electric Reliability Council June 15, 2004. www.nerc.com/docs/docs/pubs/Gas_Electricity_Interdependencies_and_Recommendations.pdf.

Gaynor, Jeff. "The Resilience Imperative: The Case for Transforming National Infrastructure and Preparedness Policy, Programs and Standards to Ensure Critical Infrastructure and National Resilience." Paper presented to 2008 TISP Corporate, Community, and Government Resilience Day conference, Washington, D.C., January 24, 2008. www.tisp.org/index.cfm?pk=download&id=11040&pid=10261.

George Mason University School of Law, Critical Infrastructure Protection Program. *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*. Arlington, VA: George Mason University School of Law, Critical Infrastructure Protection Program Discussion Paper Series, February 2007, http://cip.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf.

Geospatial Information and Technology Association. "Electric Sector Infrastructure Interdependencies." *The Geospatial Dimensions of Critical Infrastructure and Emergency Response: White Paper Series*. Geospatial Information and Technology Center, Aurora, CO: July 7, 2009. www.gita.org/ciper/InterdependenciesElectric.pdf.

Goble, Gregg, Howard Fields, and Richard Cocchiara. *Resilient infrastructure: Improving your business resilience.* Somers, NY: IBM, September 2002. www.synergisticonline.com/files/resiliancy.pdf.

Greenberg, Michael R., Michael L. Lahr, and Nancy Mantell. "Understanding the Economic Costs and Benefits of Catastrophes and Their Aftermath: A Review and Suggestions for the U.S. Federal Government." *Risk Analysts* 27, no 1. (2007): 83–96. http://policy.rutgers.edu/faculty/lahr/specialissuekatrina_4-21-06-mrg-1.pdf.

Heyman, David, and James Jay Carafano. *Homeland Security 3.0: Building a National Enterprise to Keep America Free, Safe, and Prosperous*. Washington, D.C.: CSIS, September 18, 2008. http://csis.org/files/media/csis/pubs/080918_homeland_sec_3dot0.pdf .

Homeland Security Studies and Analysis Institute. *Resilience – Concept Development: An Operational Framework for Resilience*. Arlington, VA: Homeland Security Studies and Analysis Institute, August 27, 2009. www.homelandsecurity.org/hsireports/Resilience_Task_09-01.pdf.

Hussey, Laura. "Utility Security & Resiliency: Working Together." Edison Electric Institute PowerPoint presentation, before the Federal Utility Partners Working Group (FUPWG), November 19, 2008. www1.eere.energy.gov/femp/pdfs/fupwg_fall08_hussey.pdf.

The Infrastructure Security Partnership. "White Paper for the White House Office of Critical Infrastructure Protection and Resilience Policy and Strategy: The Infrastructure Security Partnership, Infrastructure Resilience, and Interdependencies." Alexandria, VA: The Infrastructure Security Partnership, March 2010. www.tisp.org/index.cfm?pk=download&pid=10261&id=11968.

Institute of Nuclear Power Operations (INPO). "About Us." Web page. www.inpo.info/Index.html.

The Institute of Public Utilities. *Technical Assistance Briefs: Utility and Network Interdependencies: What State Regulators Need to Know*. Washington, D.C.: National Association of Regulatory Utility Commissioners, April 2005. www.naruc.org/Publications/CIP_Interdependencies_2.pdf.

Internet Security Alliance and American National Standards Institute. *The Financial Management of Cyber Risk: An Implementation Framework for CFOs*. Washington, D.C.: American National Standards Institute, 2010. www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=2489.

Jackson, Brian A. *Marrying Prevention and Resiliency: Balancing Approaches to an Uncertain Terrorist Threat*. Santa Monica, CA: RAND Corporation, 2008. www.rand.org/pubs/occasional_papers/2008/RAND_OP236.pdf.

Jackson, Scott. "The Principles of Infrastructure Resilience." Severna Park, MD: DomesticPreparedness.com, February 17, 2010. www.domesticpreparedness.com/Infrastructure/CIP-R/The_Principles_of_Infrastructure_Resilience.

Johns Hopkins University, National Center for the Study of Preparedness and Catastrophic Event Response (PACER). "National Center for the Study of Preparedness and Catastrophic Event Response." Web page. www.pacercenter.org/.

Kappenman, John. "Electric Power Grid Vulnerability to Geomagnetic Storms." 2009. www.midwestreliability.org/00_events/2009_CIP_Workshop/10._Kappenman_MRO_Dec1_2009.pdf.

Kay, Liz F., and Erica L. Green, "Thousands in Baltimore County try to cope without water: Electrical fire shuts down Towson Reservoir pumping station." *The Baltimore Sun*. April 8, 2010. http://articles.baltimoresun.com/2010-04-08/news/bal-md.co.water08apr08_1_towson-reservoir-water-service-water-tanks.

Kelic, Andjelka, Verne Loose, Vanessa Vargas, and Eric Vugrin. *Energy and Water Sector Policy Strategies for Drought Mitigation*. Albuquerque, NM: Sandia National Laboratory, 2009. http://prod.sandia.gov/techlib/access-control.cgi/2009/091360.pdf.

Meserve, Jeanne. "Sources: Staged Cyber Attack Reveals vulnerability in Power Grid." *CNN.com.* September 26, 2007. http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html.

Messmer, Ellen. "Cyberattacks: Top threat to U.S. power grid." *Network World*. Framingham, MA: June 2, 2010. www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html.

Nakashima, Ellen. "Stuxnet malware is blueprint for computer attacks on U.S." *The Washington Post*, October 2, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/10/01/AR2010100106981.html.

National Association of State Energy Officials. *State Energy Assurance Guidelines.* Washington, D.C.: National Association of Regulatory Utility Commissioners, December 2009. www.naseo.org/eaguidelines/State_Energy_Assurance_Guidelines_Version_3.1.pdf.

National Infrastructure Advisory Council. *Best Practices for Government to Enhance the Security of National Critical Infrastructures: Final Report and Recommendations by the Council*. April 13, 2004. www.dhs.gov/xlibrary/assets/niac/NIAC_BestPracticesSecurityInfrastructures_0404.pdf.

National Infrastructure Advisory Council. *Chemical, Biological, and Radiological Events and the Critical infrastructure Workforce Report and Recommendations*. January 8, 2008.

National Infrastructure Advisory Council. *Convergence of Physical and Cyber Technologies and Related Security Management Challenges.* January 16, 2007. www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport-011607.pdf.

National Infrastructure Advisory Council. *Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations*. October 14, 2008. www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf

National Infrastructure Advisory Council. *Critical Infrastructure Resilience: Final Report and Recommendations*. September 8, 2009. Appendix D contains an extensive bibliography on resilience. www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

National Infrastructure Advisory Council. *Cross Sector Interdependencies and Risk Management Guidance: Final Report and Recommendations by the Council*. January 13, 2004. www.dhs.gov/xlibrary/assets/irawgreport.pdf.

National Infrastructure Advisory Council. *Framework for Dealing with Disasters and Related Interdependencies: Final Report and Recommendations*. July 14, 2009. www.dhs.gov/xlibrary/assets/niac/niac_framework_dealing_with_disasters.pdf.

National Infrastructure Advisory Council. *Optimization of Resources for Mitigating Infrastructure Disruptions.* Non-public draft. October 2010.

National Infrastructure Advisory Council. *The Insider Threat to Critical Infrastructures.* April 8, 2008. www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.

National Infrastructure Advisory Council. *The Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States.* January 16, 2007. www.dhs.gov/xlibrary/assets/niac/niac-pandemic-wg_v8-011707.pdf.

National Infrastructure Advisory Council. *Public-Private Sector Intelligence Coordination: Final Report and Recommendations by the Council*. July 11, 2006. www.dhs.gov/xlibrary/assets/niac/niac_icwgreport_july06.pdf.

National Infrastructure Advisory Council. *Risk Management Approaches to Protection.* October 11, 2005. www.dhs.gov/xlibrary/assets/niac/NIAC_RMWG_-_2-13-06v9_FINAL.pdf.

National Infrastructure Advisory Council. *Sector Partnership Model Implementation: Final Report and Recommendations by the Council*. October 11, 2005. www.dhs.gov/xlibrary/assets/niac/NIAC_SPMWGReport_Feb06.pdf.

National Institute of Standards and Technology. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*. Washington, D.C.: U.S. Department of Commerce, January 2010. www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

National Institute of Standards and Technology Smart Grid Interoperability Panel. *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements.* Washington, D.C.: National Institute of Standards and Technology, August 2010. http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

National Security Telecommunications Advisory Committee. "Telecommunications and Electric Power Infrastructure Interdependencies." *2006-2007 NSTAC Issue Review: Active Issues*. Washington, D.C.: National Security Telecommunications Advisory Committee. www.ncs.gov/nstac/reports/2007/2006-2007%20NSTAC%20Issue%20Review.pdf.

North American Electric Reliability Corporation. *2009 Long-Term Reliability Assessment: 2009–2018.* Princeton, NJ: North America Electric Reliability Council, October 2009. www.nerc.com/files/2009_LTRA.pdf.

North American Electric Reliability Corporation. *2009 Scenario Reliability Assessment: 2009–2018*. Princeton, NJ: North America Electric Reliability Council, October 2009. www.nerc.com/files/2009_Scenario_Assessment.pdf.

North American Electric Reliability Corporation. "About NERC: Understanding the Grid." Web page. http://www.nerc.com/page.php?cid=1|15.

North American Electric Reliability Corporation. "Glossary of Terms Used in Reliability Standards." Princeton, NJ: North American Electric Reliability Council, February 12, 2008. www.nerc.com/files/Glossary_12Feb08.pdf.

North American Electric Reliability Corporation. *Reliability Concepts*. Princeton, NJ: North American Electric Reliability Council, December 2007. www.nerc.com/files/concepts_v1.0.2.pdf.

North American Electric Reliability Corporation. "Reliability Standards." Web page. www.nerc.com/page.php?cid=2|20.

North American Electric Reliability Corporation and the Electricity Sub-Sector Coordinating Council. *Critical Infrastructure Strategic Roadmap (Draft).* Princeton, NJ: NERC, 2010. http://www.nerc.com/docs/escc/ESCC_Strat_Roadmap_V3_31_Aug2010_clean.pdf.

North American Electric Reliability Corporation and the U.S. Department of Energy. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*. Princeton, NJ: North American Electric Reliability Council, June 2010. www.nerc.com/files/HILF.pdf.

North American Transmission Forum. *Tapping the collective expertise*. Brochure. July 2009. http://transmissionforum.net/forum/LinkClick.aspx?fileticket=JWbjG0Anli8%3d&tabid=40

Northeastern University, "ALERT: Awareness and Localization of Explosives-Related Threats." Awareness and Localization of Explosives-Related Threats Web page. www.northeastern.edu/alert/.

Nuclear Energy Institute. "Analysis of Nuclear Power Plants Shows Aircraft Crash Would Not Breach Structures Housing Reactor Fuel." News Release. December 23, 2002. http://www.nei.org/newsandevents/aircraftcrashbreach/.

Nuclear Energy Institute. "Key Issues: Plant Security." Web page. August 2009. www.nei.org/keyissues/safetyandsecurity/plantsecurity/.

Nuclear Energy Institute. "U.S. Nuclear Power Plants: General Statistical Information." Web page. www.nei.org/resourcesandstats/nuclear_statistics/usnuclearpowerplants/.

Nuclear Energy Institute. "Comprehensive Review (CR) Follow Up Frequently Asked Questions." n.d.

Nuclear Energy Institute. "Emergency Preparedness for Nuclear Power Plants." PowerPoint Presentation, draft, July 22, 2010.

Nuclear Energy Institute. *Fact Sheet: Emergency Preparedness Near Nuclear Power Plants.* Washington D.C.: Nuclear Energy Institute, January 2009. http://www.nei.org/resourcesandstats/documentlibrary/safetyandsecurity/factsheet/emergencypreparedness/.

Nuclear Energy Institute. *Fact Sheet: Nuclear Power Plants Designed and Constructed to Withstand Earthquakes*. Washington, D.C.: Nuclear Energy Institute, July 2009.

Nuclear Energy Institute. *Policy Brief: Nuclear Energy: Just the Facts*. Washington, D.C.: Nuclear Energy Institute, May 2008. www.nei.org/resourcesandstats/documentlibrary/reliableandaffordableenergy/brochures/justthefacts.

Nye, Erle. Letter from the chair to the National Infrastructure Advisory Council. October 27, 2009.

O'Reilly, Gerard, Huseyin Uzunalioglu, Stephen Conrad, and Walt Beyeler. *Inter-Infrastructure Simulations across Telecom, Power, and Emergency Services*. Albuquerque, NM: Sandia National Laboratory, April 2005. www.sis.pitt.edu/~dtipper/2825/Sim2.pdf.

O'Rourke, T.D. "Modern Approaches to Infrastructure Resilience." PowerPoint Presentation to University of Canterbury conference on Infrastructure Resilience. http://docs.google.com/viewer?a=v&q=cache:mXvER15XwmYJ:www.caenz.com/info/RINZ/downloads/Prestige.pdf+O%E2%80%99Rourke,+T.D.+%E2%80%9CModern+Approaches+to+Infrastructure+Resilience,%E2%80%9D&hl=en&gl=us&pid=bl&srcid=ADGEESiKVhndTJIr8zktsTSMeYAff89EbcXiATvvN1-UEwD0-eztIK4_T0FassrDKSYva3X7NBsL4dM_Hg3PZ5YEQiVbqTK3BbGMbMdKVSTx7r5QK6KjP3gdqzAl5gFXDIvsq_AF5Sz0&sig=AHIEtbQxaWvXsMI84C3pET1mD7obRqJe_g.

Ohio State University. "Supply Change Resilience Assessment & Management Tool." Center for Resilience Web page. www.resilience.osu.edu/CFR-site/scram.htm.

Partnership for Critical Infrastructure Security. *Addressing the Pandemic Influenza Threat: Preliminary Cross-Sector Readiness Assessment.* May 6, 2009.

Pommerening, Christine. George Mason University School of Law, Critical Infrastructure Protection Program. "Incorporating Resilience across the Preparedness, Protection, Response, and Recovery Spectrum: Findings from Organizational and Systems Theory and Practice." PowerPoint Presentation to Forum on Enhancing Public and Private Sector Collaboration, Alexandria, VA: April 30–May 1, 2007. http://cip.gmu.edu/research/documents/Pommerening_Incorporating_Resilience_30April07.pdf.

Prieto, Bob. *Infrastructure Resiliency: Do We Have The Focus Right?* Arlington, VA: The Infrastructure Security Partnership, November 16, 2009. www.tisp.org/index.cfm?pk=download&pid=10261&id=11838.

Pugh, Scott. "Secure Grid 2009: A DHS-DOE-DOD Joint Exercise, 9 &10 July 09." PowerPoint presentation from the 2009 Topical Symposium, *Energy Security: A Global Challenge*, hosted by the Institute for National Strategic Studies, The National Defense University, September 29-30, 2009. www.ndu.edu/inss/docUploaded/Energy_PughPPT.pdf.

Purdue University. "PURVAC: Purdue University Regional Visualization and Analytics Center." Purdue University Regional Visualization and Analytics Center (PURVAC) Web page. https://engineering.purdue.edu/PURVAC/.

Restrepo, Carlos E., Jeffrey S. Simonoff, and Rae Zimmerman. "Unraveling Geographic Interdependencies in Electric Power Infrastructure." Proceedings of the 39th Annual Hawaii International Conference on System Sciences, Track 10, 2006. http://www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2006.518

Rieger, Craig G., David I. Gertman, and Miles A. McQueen. *Resilient Control Systems: Next Generation Design Research*. Idaho Falls, ID: Idaho National Laboratory, May 2009. www.inl.gov/technicalpublications/Documents/4247208.pdf.

Rigby, Joseph M. "We can't end outages, but we can respond to them better." *The Washington Post*. August 8, 2010: C5. www.washingtonpost.com/wp-dyn/content/article/2010/08/07/AR2010080702565.html.

Rose, Adam. “Economic Resilience.” PowerPoint Presentation, Los Angeles: University of Southern California, National Center for Risk and Economic Analysis of Terrorism Events. www.resilientus.org/library/Adam_Rose_1248896517.pdf.

Rose, Adam, et al. “Business Interruption Impacts of a Terrorist Attack on the Electric Power System of Los Angeles: Customer Resilience to a Total Blackout.” *Risk Analysis* 27, no. 3(2007). Summary available at http://tdworld.com/customer_service/risk-analysis-terrorist-studies/.

Rose, A., G. Oladosu and S. Liao. "Regional Economic Impacts of Terrorist Attacks on the Electric Power System of Los Angeles: Customer Resilience to a Total Blackout." *Risk Analysis*, 27, no. 3 (2007): 513–531.

Samsa, M.E. and W. A. Buehring. *Influence of Time-Dependent Factors in the Evaluation of Critical Infrastructure Protection Measures*. Argonne, IL: Argonne National Laboratory, March 2008.

Sanders, W. H. “Progress Towards a Resilient Power Grid Infrastructure.” Proceedings of the IEEE Power & Energy Society General Meeting, Minneapolis, MN, July 25–29, 2010. www.perform.csl.illinois.edu/Papers/USAN_papers/10SAN01.pdf.

Sanders, William H. “Progress Towards a Resilient Power Grid Infrastructure.” Panel presentation, Urbana, IL: University of Illinois, Center for the Trustworthy Cyber Infrastructure for the Power Grid. www.perform.csl.illinois.edu/Papers/USAN_papers/10SAN01.pdf.

Sandia National Laboratory. *A Framework for Critical Infrastructure Resilience Analysis.* Albuquerque, NM: Sandia National Laboratory. www.sandia.gov/mission/ste/stories/2009/September%202009/individual%20files/Snyder-09.pdf.

Schuh, Mike. “Baltimore Co. Raises Questions After Water Outage.” *Channel 13 WJZ*. April 8, 2010. http://wjz.com/local/Northern.Baltimore.County.2.1619774.html.

Sheffi, Yossi. “Building a Resilient Organization.” *The Bridge* 37, no. 1 (2007): 30–36. Washington, D.C.: National Academy of Engineering. http://web.mit.edu/sheffi/www/documents/Bridge-v37n1.pdf.

South Texas Project Nuclear Power Plant. “STP Nuclear Power Plant: Facts and Stats.” Web page. www.stpnoc.com/FYI.htm.

Stevens Institute of Technology. “Port Security: National Center for Secure & Resilient Maritime Commerce.” National Center for Secure and Resilient Maritime Commerce Web page. www.stevens.edu/csr/.

Sutherland, J.J. “Thad Allen and Lessons Learned from the Gulf Oil Spill.” *NPR*. September 9, 2010. http://www.npr.org/blogs/thetwo-way/2010/09/08/129726292/admiral-thad-allen-and-lessons-learned-from-the-gulf-oil-spill

Syracuse University. “Resilience and Security: Comprehensive Bibliography.” Institute for National Security and Counterterrorism Web page. http://insct.syr.edu/projects/resilience-and-national-security/research/.

Tennessee Bar Association. “May 2010 Floods.” PowerPoint presentation. http://www.tba.org/volunteer/floodguide_051010.pdf.

Tennessee Emergency Management Agency. “Bredesen Announces Disaster Declarations for 3 More Tennessee Counties.” Press release. May 7, 2010. http://news.tennesseeanytime.org/node/5087.

Tennessean staff reports. “Obama declares Nashville a disaster area.” *The Tennessean*, May 4, 2010. http://www.tennessean.com/article/20100504/NEWS01/100504018/President-Obama-declares-Nashville-a-disaster-area.

Tierney, Kathleen. *Disaster Response: Research Findings and Their Implications for Resilience Measures*, *CARRI Research Report 6*. Boulder, CO: Oak Ridge National Laboratory, Community & Regional Resilience Initiative (CARRI), March 2009. www.resilientus.org/library/Final_Tierney2_dpsbjs_1238179110.pdf.

Tkachenko, Maxim. “Power plant ‘terror’ attack kills 2 in Russia.” *CNN.com*. July 21, 2010. www.cnn.com/2010/WORLD/europe/07/21/russia.station.attack/index.html.

U.S. Army Corps of Engineers. *After-Action Report: May 2010 Flood Event Cumberland River Basin*. July 21, 2010. http://www.lrn.usace.army.mil/LRN_pdf/AAR_May_2010_Flood_Cumberland_Draft_V7_21.pdf.

U.S. Department of Energy. *Energy: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan* (Redacted). Washington, D.C.: U.S. Department of Energy, May 2007. www.oe.energy.gov/DocumentsandMedia/Energy_SSP_Public.pdf.

U.S. Department of Energy. *Nuclear Energy Research and Development Roadmap: Report to Congress*. Washington, D.C.: DOE, April 2010. www.nuclear.gov/pdfFiles/NuclearEnergy_Roadmap_Final.pdf.

U.S. Department of Energy. *The Smart Grid: An Introduction*. Washington, D.C.: Department of Energy, 2008. www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf.

U.S. Department of Energy Energy information Administration. “Electric Power Industry Overview 2007: The Changing Electric Power Industry.” http://www.eia.doe.gov/cneaf/electricity/page/prim2/toc2.html#change

U.S. Department of Energy Energy Information Administration. “Electricity End Use, Selected Year, 1949–2009.” http://www.eia.gov/emeu/aer/pdf/pages/sec8_37.pdf.

U.S. Department of Energy Energy Information Administration. “Energy Explained: Your Guide To Understanding Energy.” http://tonto.eia.doe.gov/energyexplained/index.cfm

U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, Infrastructure Security and Energy Restoration. *Hardening and Resiliency: U.S. Energy Industry Response to Recent Hurricane Seasons*. Washington, D.C.: U.S. Department of Energy, August 2010. www.oe.netl.doe.gov/docs/HR-Report-final-081710.pdf.

U.S. Department of Homeland Security. “Comprehensive Reviews.” Web page. www.dhs.gov/files/programs/gc_1228760276865.shtm.

U.S. Department of Homeland Security. “Homeland Security Centers of Excellence.” Web page. www.dhs.gov/files/programs/editorial_0498.shtm.

U.S. Department of Homeland Security. “Nuclear Sector Comprehensive Reviews.” Web page. www.dhs.gov/files/programs/gc_1189794852731.shtm.

U.S. Department of Homeland Security, Federal Emergency Management Agency, National Incident Management System. “NIMS.” Web page. www.fema.gov/emergency/nims.

U.S. Department of Homeland Security, Federal Emergency Management Agency, National Response Framework (NRF) Resource Center. “NRF Resource Center.” Web page. www.fema.gov/emergency/nrf/.

U.S. Department of Homeland Security, Federal Emergency Management Agency. *National Response Framework: Nuclear/Radiological Incident Annex*. Washington, D.C.: Federal Emergency Management Agency, 2008. www.fema.gov/pdf/emergency/nrf/nrf_nuclearradiologicalincidentannex.pdf.

U.S. Department of Homeland Security. *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency.* Washington, D.C.: U.S. Department of Homeland Security, 2009. www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

U.S. Department of Homeland Security. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*. Washington, D.C.: U.S. Department of Homeland Security, February 2010. http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

U.S. Department of Homeland Security, Office of Infrastructure Protection, Sector Specific Agency Executive Management Office. "National Infrastructure Protection Plan." Presentation, May 5, 2009. www.r-tac.org/DHS_OIP.pdf.

U.S. Federal Energy Regulatory Commission. "Order Approving Stipulation and Consent Agreement: Florida Blackout." 129 FERC 61,016, Docket No. IN08-5-000, October 8, 2009. www.nerc.com/files/Order_FPL_Settlement_10082009.pdf.

U.S. Government Accountability Office. *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed.* Washington, D.C.: U.S. Government Accountability Office, July 2010. www.gao.gov/new.items/d10628.pdf.

U.S. Government Accountability Office. *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, *GAO-10-296*. Washington, D.C.: U.S. Government Accountability Office, March 2010. www.gao.gov/new.items/d10296.pdf.

U.S. Nuclear Regulatory Commission. "Frequently Asked Questions About NRC's Design Basis Threat Final Rule." Web page. www.nrc.gov/security/faq-dbtfr.html.

U.S. Nuclear Regulatory Commission. "Nuclear Security and Safeguards." Web page. www.nrc.gov/security.html.

U.S. Nuclear Regulatory Commission. "Physical Protection." Web page. www.nrc.gov/security/domestic/phys-protect.html.

U.S. Nuclear Regulatory Commission. "Security Spotlight." Web page. May 2007. www.nrc.gov/reading-rm/doc-collections/fact-sheets/security-spotlight/index.html.

U.S. Nuclear Regulatory Commission. *Strategic Plan: Fiscal Years 2008-2013(NUREG-1614, Vol. 4)*. Washington, D.C.: U.S. Nuclear Regulatory Commission, 2008. www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1614/v4/sr1614v4.pdf.

U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. U.S.-Canada Power System Outage Task Force: April 2004. https://reports.energy.gov/BlackoutFinal-Web.pdf.

University of Maryland, National Consortium for the Study of Terrorism and Responses to Terrorism Web page. "START: National Consortium for the Study of Terrorism and Responses to Terrorism." www.start.umd.edu/start/.

University of North Carolina, National Center for Natural Disasters, Coastal Infrastructure and Emergency Management. "The Department of Homeland Security Center of Excellence—Natural

Disasters, Coastal Infrastructure and Emergency Management." Web page. http://hazardscenter.unc.edu/diem/.

University of Southern California, National Center for Risk and Economic Analysis of Terrorism Events. "National Center for Risk and Economic Analysis of Terrorism Events." Web page. http://create.usc.edu/.

White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington, D.C.: White House, 2009. www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

White House. *National Security Strategy.* Washington, D.C.: White House, May 2010. www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

White House. *National Strategy to Secure Cyberspace.* Washington, D.C.: White House, February 2003. www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.