NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

PRINCETON FORRESTAL VILLAGE, 116-390 VILLAGE BOULEVARD, PRINCETON, NEW JERSEY 08540-5731

THE ELECTRICITY SECTOR RESPONSE TO THE CRITICAL INFRASTRUCTURE PROTECTION CHALLENGE MAY 2002

Introduction

The business, technological, and national security environment in which North America's electric power infrastructure is operated and maintained is dramatically changing. New threats and vulnerabilities to the continued reliability and integrity of our infrastructure, particularly our electronic systems, are rapidly emerging. The electricity sector has a long history of working together to assure the reliability of the North American electric system. Consequently, it takes seriously[*] any new issues that affect that reliability. An approach to action that the electricity sector could feasibly take is to:

1. Recognize what the industry already does well because of its cooperative structures, policies, and processes.
2. Identify what has changed in our environment by extending what we already do well in critical infrastructure protection/asset risk management to include emerging physical and electronic threats.
3. Build on existing processes and structures already in place to address new issues (use existing roles modeled in the North American Electric Reliability Council (NERC), regional councils and individual organizations).
4. Broaden industry learning and cooperation with others in the electricity sector to improve efficiency of implementation (advance industry cooperation through partnerships, reliability councils, and trade association initiatives).
5. Work cooperatively with government, those within our industry, and other business sectors to identify and address roles, interdependencies, obstacles and barriers (what is the role of government, research and development, legal, and policy issues, etc.).

[*] This Response and the Approach to Action document mentioned in this Response were developed by the dedicated efforts of the 40 members of NERC's Critical Infrastructure Protection Advisory Group. This group provides guidance to the electricity sector regarding threats to and vulnerabilities of the electric power systems of North America. Activities encompass both physical and electronic protection, including monitoring, detection, training, and exercises. Representation has included utility members from NERC regions, a power marketer, an independent power producer, the American Public Power Association, Canadian Electricity Association, Edison Electric Institute, Electric Power Supply Association, National Rural Electric Cooperative Association, the Electric Power Research Institute, the Department of Energy, Federal Bureau of Investigation, National Infrastructure Protection Center, the Critical Infrastructure Assurance Office and NERC staff. The advisory group's efforts reflect the industry's serious commitment to critical infrastructure protection.

How does the electricity sector define critical infrastructure protection? *Critical infrastructure protection means safeguarding the essential components of the electric infrastructure against physical and electronic threats in a manner consistent with appropriate risk management, with both industry and industry-government partnerships, while sustaining public confidence in the electricity sector.*

Overview of the Approach

Assuring the delivery of electricity over the nation's electric infrastructure is our industry's business on a daily basis. Because electricity is the foundation for our society's core activities, the expectations of our customers and the public create a compelling case for our industry members to exercise due diligence in protecting and managing both our physical and electronic assets critical to reliability and the integrity of their electric systems.

The North American electric systems are highly interconnected. Consequently, there are three levels of service assurance activity, developed over years as our industry responded to natural disasters, malicious acts and other crises.

- NERC provides coordination for reliability nationally and internationally with the United States, Canada, and Mexico, while the individual utilities and the regional councils work with state and local governments.
- The industry's history of interconnectedness and interdependency between regions and utilities has engendered cooperation between utilities and regions in times of crisis and emergencies. Consequently, not only does a utility look to assure its own service capability, it looks to its neighbors to offer or request support. The industry's demonstrated ability to respond to emergencies shows the value of mutual aid programs and this reciprocal cooperation.
- Interdependencies between other infrastructures and the electricity sector are complex and require continued review and assessment. Individual electric utilities have over the years developed working relationships with local telecommunications, oil and natural gas suppliers, and other infrastructures as well as local and state government emergency service providers. The importance of these local relationships was recognized and reinforced during preparations for the Y2K roll over. In addition, the federal government and some states are identifying interdependencies and providing coordination for the industry in structuring statewide and regional emergency response plans.

This document describes a general approach to action implicit in the plans and programs industry members, NERC, and its regional councils take to assure service. Individual programs implemented and choices for action depend on each organization's assessment of its own individual threats, vulnerabilities, potential consequences, local community and customer expectations, and tolerance for risk. The more information made available about these considerations, the better informed the decisions will be by each organization and the industry as a whole, particularly as new threats and vulnerabilities emerge and are clearly identified.

This approach to action is organized around a common security model that includes the following categories:

- Identifying critical services and the assets supporting them
- Assessing vulnerabilities, including review of policies, procedures and standards
- Performing risk assessments, including review of mitigation measures
- Writing and testing recovery and restoration plans
- Monitoring and periodically updating assessments
- Sharing information, educating and maintaining awareness
- Coordinating activities within the electric sector
- Understanding the interdependencies across all critical sectors
- Identifying and supporting research and development
- Recognizing legal and regulatory issues and other challenges to implementing CIP programs

What specific challenges need to be addressed in critical infrastructure protection within the electricity sector?

- *Awareness – building a recognition and appreciation for emerging threats and vulnerabilities, plus explicitly defining physical and information security as an essential component of the electric industry definition of "reliability."*
- *Technology – managing a growing complexity of electronic devices, and understanding and incorporating technology risk into broader business risk management processes.*
- *Sharing – enhancing existing communications within organizations (e.g. IT, Operations, and Security), among electricity sector participants, across interdependent business sectors, and in liaison with governmental agencies.*
- *Approach – extending and building on structures, policies and processes already in existence to address emerging physical and electronic threats.*
- *Restructuring – ensuring that critical infrastructure protection efforts do not impede industry restructuring, and that restructuring is supportive of critical infrastructure protection initiatives.*
- *Roadmap – delineating appropriate strategies, programs and processes for establishing and executing security initiatives.*

Historical Commitment of the Industry

The North American Electric Reliability Council (NERC) has been asked on a number of occasions during the past decade to serve as the electricity sector's primary point of contact for issues relating to national security. Since the early 1980s, NERC has acted to address the electromagnetic pulse phenomenon, vulnerability of electric systems to state-sponsored, multisite sabotage and terrorism, Y2K rollover impacts, and now the rapidly evolving threat of electronic intrusion as well as physical attack. At the heart of NERC's efforts has been a commitment to work with various federal government agencies to reduce the vulnerability of interconnected electric systems to such threats.

The Report of the President's Commission on Critical Infrastructure Protection (PCCIP) in October 1997 led to a May 1998 Presidential Decision Directive (PDD-63). PDD-63 called for government agencies to become involved in the process of developing a National Strategy for Critical Infrastructure Assurance, and to seek voluntary participation of private industry to meet common goals for protecting the country's critical infrastructure through public-private partnerships. The PCCIP specifically commended NERC as a model for information sharing, cooperation, and coordination between the private sector and government. In September 1998, the Secretary of Energy wrote to the NERC Chairman seeking NERC's assistance, on behalf of the Electricity Sector, in developing a program for protecting the continent's critical electricity sector infrastructure. Responding to the U.S. Department of Energy's critical infrastructure protection initiative, NERC agreed to participate as the Electricity Sector coordinator. This document focuses on the approach that NERC and the United States, Canadian, and Mexican members of the electricity sector may take in playing an active role in the full-range of critical infrastructure protection (CIP)/asset risk management activities.

What has the electricity sector accomplished since PDD-63?

- *Created an active CIP Advisory Group, with representation from a broad spectrum of North American utility members, other utility-industry organizations and government. The Advisory Group reports to the NERC Board of Trustees. This Group also receives input from other industry related security committees (i.e. EEI, CEA, APPA and NRECA).*
- *Enhanced partnerships with federal government entities, especially the FBI, NIPC, DOE, the National Labs, CIAO, Rural Utility Services, and Canadian counterpart organizations.*
- *Developed closer working relationships across utility-industry organizations, especially between NERC, EEI, AGA, APPA, NRECA, and EPRI.*
- *Established an electricity sector ISAC that gathers incident information, relays alert notices, and includes daily briefs with the FBI/NIPC and electric grid operators around the country. Created the Indications, Analysis and Warning Program that train utilities on incident reporting and alert notification procedures.*
- *Created a utility-CEO security committee to enhance planning, awareness and resource allocation.*
- *Conducted numerous industry outreach efforts (i.e. brochures, forums and presentations) targeting executive management, security personnel, operations staff, government representatives, and equipment suppliers, which address simple topics (i.e. security awareness), to general topics (i.e. vulnerability assessment lessons learned), to technical topics (i.e. digital process controls).*
- *Developed security reference documents for the electricity sector,*

including an "Approach to [security] Action", "Security Guidelines" and "Threat Alert Levels and Response Guidelines (for physical and cyber events)."

- *Established security programs, like EPRI's Enterprise Infrastructure Security Program that developed for members, policy and procedure guides, procurement guides, power line and power plant security primers, and risk management guides. The industry has also hosted numerous guest speakers in different forums to further educate industry members on emerging security topics, new decision tools and techniques.*
- *Conducted threat and vulnerability assessments on numerous internal operations and electric grid operations, consolidating lessons learned and encouraging utilities to share their experiences with other industry members.*
- *Built working relationships with cross-sector organizations, especially the PCIS and other industry ISAC's.*
- *Developed several working teams to address industry-wide issues, like information sharing, encryption and inventory of critical components.*

Elements of the Electricity Sector's Approach to Action

The Approach to Action document is organized around a four-tier security model of actions to counter physical and electronic threats: avoidance (such as use of policies, procedures and awareness programs), assurance (such as periodic re-evaluations of risk), detection (such as monitoring, reporting and analysis of issues), and recovery (investigation, restoration and sharing of lessons learned). The principle elements of this Approach to Action can be grouped into the following categories:

A. Identification of Critical Services and Assets

The goal of risk management is to mitigate potential consequences at a cost commensurate with the potential loss. Critical services or service levels are identified based on mission operational criticality and public and customer expectations and needs. Priorities are generally given to public safety and confidence. Utilities usually work with their customers, state and local government, and the federal government to identify what services and service levels are deemed critical. Once identified, the assets that support them can be identified and programs put in place to manage the known risk.

Assessing security risk begins with a clear delineation of the critical functions that sustain the mission and functionality of operations and service, followed by identifying the critical assets that support them. This assessment reveals why these assets are important (i.e. what attributes make them important), and their relative measure of criticality (i.e. dimensions that define the consequences of asset loss or compromise). Physical and electronic assets are considered and can include the information infrastructure, hardware, software, data and information, people, documentation, and supplies. Assessments consider both the dollar value of the asset, and the value of the asset relative to the mission it supports.

Working with customers and institutions representing the public interest, the following considerations may help to determine what is included in a list of critical assets for the electrical power supply system infrastructure.

National Security – Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the ability of the United States, Canadian or Mexican military or government to satisfy their critical mission in support of national military or civil security?

Public Health and Safety – Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten public safety and health, and/or the environment of the United States, Canada or Mexico?

Economic Security – Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the economic security of the United States, Canadian or Mexican economy?

Regional, National, and North American Electrical Grid Reliability – Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten regional, national, or North American electrical grid reliability?

Generation, Transmission and Distribution – Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the supply or delivery of power necessary to adequately serve the regional, national, or North American electric demand?

Critical Control Systems – Will the loss or compromise of operational systems disrupt or otherwise threaten control of the generation, transmission, or distribution of electricity in real time?

Essential Business Systems – Will the loss or compromise of operational systems disrupt or otherwise threaten operational reliability and business systems that could have a significant impact on corporate or government financial operations?

B. Vulnerability Assessments

Evaluating physical and electronic vulnerabilities can provide several benefits:

- Identifies practices and situations that increase risk.
- Discovers activities and practices that reduce risk.
- Distinguishes between strategic and tactical efforts for managing consequences.
- Links business unit decisions that can affect the entire enterprise.

- Provides a rationale for prioritizing follow up work and allocating resources when viewed from the perspective of asset criticality and threat.
- Offers a basis for identifying awareness and training issues.

Assessing security risk includes assessing vulnerabilities by reviewing paper records (e.g. what rules/documentation are in place), conducting interviews (e.g. how do people function/feel regarding security), visiting sites (e.g. how are systems installed and operated), and performing tests (e.g. how do systems and people respond to attacks).

When considering this approach, the following factors may be considered in assessing physical and electronic vulnerabilities.

Network Architecture – Network topology, principal information assets, encryption communication protocols, access controls, intrusion detection and alarm reporting.

Penetration Testing – Tests that emulate the outsider threat, the insider threat, and specific exploits such as social engineering and war dialing.

Physical Security – Access controls, intrusion detection devices and associated alarm reporting and displays, communications equipment, lighting, power sources, and protective force.

Physical Asset Analysis – Asset utilization, system redundancies, and interdependencies with other infrastructures.

Operations Security – Denying adversary access to sensitive and non-sensitive information that might inappropriately aid or abet any individual or organization's disproportionate influence over markets or system operations.

Policies and Procedures – Business processes are reviewed to 1) address the key factors affecting security, 2) enable effective compliance, implementation and enforcement, 3) reference or conform to established standards, 4) provide clear and comprehensive guidance, and 5) effectively address roles, responsibilities, authorities and accountabilities.

C. Risk Assessment and Management

Critical infrastructure assurance has always been recognized by industry as a risk management process. Assessing and managing security risks in today's environment, however, means a new way of looking at the issues included in an enterprise-wide risk assessment. That broader perspective, besides recognizing the usual business orientated risk factors, may include issues such as:

- Financial risk
- Environmental risk
- Safety risk

- Supply risk (e.g. fuel, water, replacement parts, etc.)
- Construction and contractor risk
- Insurance risk
- National and international political and regulatory risk
- Brand equity risk
- Security risk

A risk management program generally includes varying levels of investments in an entire range of actions from prevention/deterrence to incident management and mitigation to response and recovery. Decisions on where in this range to invest usually depend on knowledge of threat or vulnerability, feasibility of investment, and predictability of consequence. For example, some utilities serving geographic areas prone to natural disasters have become extremely skilled at crisis response, and recovery and restoration, because natural disasters cannot be prevented, nor all their consequences predicted.

Another form of risk management may include employment background screening with possible consideration to periodic or on-going screening programs. Effective screening can prevent or deter negligent hiring, employee theft and drug use. Such screening may provide considerations for new employees, promoted employees, contractors and vendors, especially those who either work at critical facilities or in direct support of critical services. Additional considerations may be needed for non-national citizens.

D. Recovery and Restoration

The recovery and restoration components of the Approach to Action document refer to activities that develop plans for managing an emergency from the moment it occurs, managing efforts to restore systems to a normal state, conducting simulation drills, tracking lessons learned and sharing best practices. Recovery and restoration efforts vary for physical and electronic assets.

Effects from isolated intentional attacks on physical facilities are only marginally different from those of natural events. This analogy applies to the nature of the damage inflicted and to the ability to begin repair operations. There are, however, significant differences between natural disasters and well-planned, coordinated, and widespread intentional attacks on physical facilities. For example, attackers could focus on several of the most difficult to defend or repair targets simultaneously. However, in contrast to the testing of electronic system security, the testing of physical system security is a mature and well-understood discipline. Tabletop exercises are often used to plan for natural disasters: these techniques have proven effective in testing response and recovery procedures, and are applicable to security issues as well.

Most electric organizations rely on computerized systems for billing, system operation, and for internal management functions. Where the competitive electricity market depends on the electronic exchange of bids and offers the reliance is even greater and more time-critical. A plan to restore business operations following an electronic disruption incident could mean the difference between commercial success and failure. Effective electronic recovery and restoration plans may consider the possibility of various types of attacks. Electronic crimes may require other special handling, such as law enforcement accommodations for preserving computer evidence. This accommodation may also affect timely restoration of services or facilities.

E. Monitoring and Updating.

Monitoring and recording systems enable the identification of suspected and actual incidents for investigative follow-up. Real-time monitoring permits timely organizational response to physical and electronic threats. Timely monitoring and response are critical factors to maintaining operational integrity and availability.

Physical security real-time monitoring efforts can be quite broad, and may consider such things as reports from access control systems, video surveillance, voice recordings, facility inspections, reports of credible threats by employees, and external threats reported by law enforcement authorities.

Electricity supply and delivery organizations may need to correlate unique events from several different log sources to identify patterns that individually may not represent a threat but in combination could indicate a particularly harmful threat/incident. The number of sources and the potentially voluminous log data may require automated real-time monitoring and alerting efforts.

Groups analyzing monitored information may need to report a threat issue to internal management, internal security, and several external organizations such as NIPC and law enforcement. Electric supply and delivery organizations can consider participatory reporting through electric industry reliability programs (e.g., Electricity Sector 'Information Sharing and Analysis Center', or ISAC) and cooperative electric industry - governmental programs (e.g., Indications, Analysis, and Warning program).

F. Information Sharing, Education and Awareness

A comprehensive response to an emergency among electric industry organizations depends, in part, on the timely sharing of threat and vulnerability information. The electric industry has well developed reporting and alert channels, which have evolved over the last 50 years. Because the human and physical infrastructure already exists, the sharing of information and incident reporting within the industry for electronic and physical security incidents that affect the reliability of the electric system can be built on currently existing structures and procedures. Several security reporting initiatives are underway:

- NERC's "Reliability Authority Information System" is being expanded for electronic incident reporting.
- NERC and the National Infrastructure Protection Center have implemented the 'Indications, Analysis and Warning' reporting and alert system. This system can channel incident reports to NERC's Electricity Sector ISAC or the FBI's National Infrastructure Protection Center (NIPC). These same channels can also be used by the ISAC and NIPC to provide alert notifications to industry members.
- NERC manages the Critical Infrastructure Protection Information System (CIPIS) for non-control room communications.

- Industry members individually, at their option, may participate in the FBI's 'InfraGard' program or in other information sharing programs available throughout private industry, which include reporting and alert mechanisms.
- All critical infrastructure sectors in conjunction with the Office of Homeland Security are currently reviewing standardized threat alert levels. In addition, Electricity Sector organizations are developing response guidelines for each alert level, which delineate actions to actively countermeasure anticipated threats.
- The Electricity Sector ISAC is working with other infrastructure ISAC's (e.g. gas, oil, chemical) to ensure effective cross-industry communications occur relative to security incidents and alert notices.

Outreach to raise awareness and educate electric industry leadership, operations, and security professionals can be an important tool in dealing with electronic and physical security problems. An organization's best defense is employees who understand and support security policies and procedures. An employee awareness program educates employees on actions that reduce security risks, such as the need to select, protect and change "good" passwords, not add unauthorized modems, shred documents that could compromise security, and raise employee awareness about the risks of social engineering. NERC and the Edison Electric Institute are working on a series of voluntary security guidelines for the industry that describe general approaches, considerations, practices and planning philosophies that can be applied in protecting electric infrastructure systems.

To address and resolve a security issue requires that an organization and its employees have awareness, understanding, and acceptance of the existence of a problem. Subsequent education on roles and responsibilities and use of tools and execution of proper controls is then much better received and internalized. Awareness and education also engages recipients as problem solvers, capturing existing knowledge, expertise, and creativity, thus, broadening and deepening the available resource.

Awareness and outreach to the senior level of management of individual organizations and regional councils provides additional information for making more informed business choices on identifying and managing emerging risks. NERC has rolled out an awareness program, specifically targeting CEOs, CIOs, operations managers, and the NERC Board of Trustees.

G. Coordination within the Electric Industry

Electricity supply and delivery organizations continue to cooperate and depend on coordinated operating systems as well as resource sharing efforts during emergencies. Both informal and formal mutual assistance programs exist. Some programs are for specific industry groups (e.g. Edison Electric Institute – Mutual Assistance Program, Federal Response Plan for municipal utilities), and other programs are for specific regions (e.g. Mutual Emergency Material Support for southeastern utilities). In addition, NERC maintains a database of bulk electric system spare transformers in North America, and a proper names and contacts database of bulk electric supply and delivery facilities.

H. Interdependencies

Infrastructure interdependency refers to the physical, electronic, and new economy (e-commerce) linkages within and among the critical infrastructures—electric, gas, oil, coal, telecommunications, banking and finance, transportation, water systems, emergency services, government services, manufacturing and food/agriculture. These linkages vary significantly in terms of scale and complexity, and typically involve a large number of system components.

When considering this element of the approach, identifying and analyzing linkages requires a detailed understanding of how the components of each infrastructure and their associated systems depend on and are supported by each of the other infrastructures. In addition, not all aspects of one infrastructure's dependence on another may be understood or appreciated and may need further investigation.

For example, much new electric generation depends on natural gas, and gas itself may depend on electric power for control systems, storage operations, compressor stations, and telecommunications for transmitting operational signals.

Although the electricity sector has "hands-on" experience identifying and working with interdependencies at the local and regional level in some parts of the North America, work to broaden understanding of interdependencies at the local, regional levels, and across infrastructure sectors has begun, particularly with participation in the Partnership for Critical Infrastructure Security (PCIS).

I. Research and Development (R&D)

Research and development may need to be increased to more adequately address the new challenges facing the nation's critical infrastructures. These challenges encompass physical and electronic information security, as well as intrinsic threats from the growing, and changing, complexity of, and interdependence among, infrastructures. Meeting these challenges may require new resources, a new examination of R&D requirements and gaps in the security model (avoidance, assurance, detection, and recovery), and a new partnership among government, industry, and academia.

Security issues related to process control systems (SCADA, EMS, DCS, PLC and smart field devices) illustrate potential R&D opportunities. Encryption, firewalls and intrusion detection systems designed for information technology applications are not easily backfitted into process control systems, which inherently need fast response rates and use different communication protocols. In this case, research is needed to better understand the limits to technology and to ideas, and create new approaches to solving these problems.

J. Legal Issues and Challenges Associated with CIP

To ensure that North America's critical electric infrastructures are protected, the government must work closely with the electricity sector, which needs assistance in promoting cooperation and sharing in the following areas:

- Under the Freedom of Information Act ("FOIA"), there is a presumption that records in the possession of agencies and departments of the executive branch of the U.S.

Government are accessible by the public. Recognizing the legitimate need to restrict disclosure of some information, and to promote cooperation with statutes and regulations, however, Congress has provided for numerous exemptions under which information is not subject to disclosure. Currently, it is not sufficiently established that any of the existing FOIA exemptions provide the certainty of protection in disclosing threat and vulnerability information.

- Businesses need protection from unintended restrictions placed by Federal and state antitrust laws on critical information sharing. Federal antitrust law and policy is concerned with furthering competition in the marketplace. Certain types of agreements, cooperative arrangements, and information sharing amongst industry participants may have anti-competitive effects. These anti-competitive effects may exist where the agreements (or, collaborative models) have the effect of raising prices or reducing outputs – irrespective of intent. The mere cooperation of large segments of various markets may raise questions by non-participating members in relevant markets, agencies, and other non-government organizations – thus, increasing the risk to participants.
- Businesses need to be shielded from legal liability for a wide range of risk management planning activity – such as performing risk assessments, testing infrastructure security, or sharing certain threat and vulnerability information. Issues that need to be addressed include: defining duties of care for management, directors and officers; limiting liability for owners/operators of critical infrastructure facilities; facilitating strategies that support electronic-security/liability insurance availability; developing damage caps for downstream harm resulting from cascading impacts; limiting liability from inconsistent requirements on national or global companies.
- The electronic-threat defensive expenditures of electric power organizations need a consistent treatment for federal corporate income tax purposes. In particular, will firms be allowed to expense these amounts or will they be required to amortize them, even if firms do not want to do so? To the extent that firms can expense such expenditures, they are more willing to undertake them. This is especially true if, in some circumstances, government authorities may have some reason for wanting a firm to erect higher defenses than the firm’s management or board thought its fiduciary responsibilities required. If the government wants increased security expenditures by industry, presumably favorable rather than adverse tax treatment would be part of a larger government policy toward that end.

What useful support can the Federal government provide to promote infrastructure protection?

- *Trust – a formal and recognized structure to ensure that potentially sensitive information is shared quickly and appropriately between industry and government, including United States, Canadian and Mexican federal governments, as well as state, provincial and local governments.*
- *Information – timely, actionable information on the nature and characterization of threats, as well as relevant warnings to which it may have unique access.*
- *R&D – investment in basic research that natural market forces cannot adequately support, such as evaluation of the movement*

toward a digital society and development of strategies and products to better manage an increasingly interconnected work environment.

- *Facilitation – forums to encourage and facilitate communication and dialogue on supporting development, practices and technologies, common to all the critical infrastructures.*
- *Update – work with industry to identify and address conflicting public policy requirements, developed over time, which unintentionally impedes protection of critical infrastructures.*
- *Streamline – work with industry to reduce procedural inefficiencies to cooperate with government –an example of which are the multiplicity of government reports now required for electric system operators who may be in the midst of bringing back electric service for customers and the public.*
- *Outreach – support various educational and awareness programs such as DOE's Infrastructure Assurance Outreach Program that provide opportunities for businesses to conduct initial security assessments that normally would not be funded by the business, yet yield essential security knowledge which provides justification for business to act upon.*
- *Coordination – work to develop consistency between Federal and State efforts, for example in treatment of FOIA, and in operation of Federal and state Homeland Security programs.*
- *Funding – assist Federal and state regulatory agencies in providing cost recovery mechanisms for protecting critical infrastructures in the electricity sector.*
- *Response Plans – establish national means to defend electricity sector critical assets from nation-state threats.*

Conclusion

The application of new technologies, and the changing political and social landscape around the world have multiplied threats and vulnerabilities — both physical and cyber, both electric and electronic. The nature and extent of these threats to reliable service, however, are further magnified by new and growing national and international tensions. The September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon had far reaching impacts on services and systems that underpin every aspect of our lives. The Department of Commerce's Critical Infrastructure Assurance Office recently noted, "That the loss of telecommunications services can impede financial service transactions and delivery of electric power is no longer an exercise scenario. There can be no e-commerce without 'e' electricity."

For good business reasons, as well as considerations of national security, individual institutions will need to respond to these threats by managing and appropriately protecting their own systems and their connections to others, to assure reliability and integrity of the North American electric transmission systems and to maintain public confidence in them. Assessment of risk to these electricity supply and delivery systems will need to include consideration of dependencies on others, and enhanced protection will need to include enhanced cooperation with others.

Taken as a whole, this approach can help to maintain the industry’s security, the confidence of the industry’s customers, and the confidence of the general public in the reliability and integrity of North America’s electric supply and delivery systems, and the electric infrastructure.