

**Testimony of
Michehl R. Gent, President and Chief Executive Officer
North American Electric Reliability Council**

**Hearing Before the United States Senate
Committee on Governmental Affairs**

May 8, 2002

**SECURING OUR INFRASTRUCTURE: PRIVATE/PUBLIC
INFORMATION SHARING**

Summary

- The electric industry operates in a constant state of preparedness. Planning, training, and operating synchronous (non-switchable) grids prepares the electric industry for natural disasters such as earthquakes, floods, tornados, energy emergencies, and attacks of sabotage and terrorism.
- The North American Electric Reliability Council (NERC) serves as the electric industry's contact and coordinator in the United States and Canada for bulk electric system security matters and is the Electricity Sector's Information Sharing and Analysis Center (ES-ISAC).
- NERC has elevated critical infrastructure protection to be the focus of a high-level advisory group comprised of all ownership segments in the electric industry. The Critical Infrastructure Protection Advisory Group (CIPAG) reports directly to NERC's Board of Trustees.
- Infrastructure protection is a high priority for those who operate electric systems. CIPAG is the electric industry's primary organization for coordinating with government agencies and for oversight of NERC activities relating to critical infrastructure protection.

Recommendations

- Provide a way for sponsoring agencies, such as the FBI and DOE, to increase the number of industry personnel with security clearances. Private industry input is needed for credible vulnerability assessments.
- Provide inexpensive, effective, secure communications tools for industry participants in infrastructure ISACs.
- Provide limited, specific exemptions from the Freedom of Information Act restrictions for certain sensitive information shared by the private sector with the federal government. Provide narrow antitrust exemption for certain related information-sharing activities within the industry. S. 1456 achieves this result.

- Adopt the reliability legislation recently passed by the Senate as part of the comprehensive energy bill.

Background

My name is Michehl R. Gent, and I am President and Chief Executive Officer of the North American Electric Reliability Council. NERC is a not-for-profit organization formed after the Northeast blackout in 1965 to promote the reliability of the bulk electric systems that serve North America. NERC comprises ten Regional Reliability Councils that account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

NERC works with all segments of the electric industry ? investor-owned utilities; federal power utilities; rural electric cooperatives; state, municipal, and provincial utilities; independent power producers; and power marketers ? as well as end-use customers, to “keep the lights on” by developing and encouraging compliance with rules for the reliable operation of the electric system. NERC also works closely with the federal government agencies to ensure that the nation’s critical infrastructure protection programs are implemented throughout the electric industry.

I am responsible for directing NERC’s activities both within the electric industry and between the electric industry and the federal government as these activities relate to physical and cyber terrorism of the electric systems of North America. NERC has served on a number of occasions as the electric utility industry’s primary point of contact for issues relating to national security. This began in the early 1980s when NERC became involved with the electromagnetic pulse phenomenon. Since then, NERC has worked with the federal government to address the vulnerability of electric systems to state-sponsored, multi-site sabotage and terrorism, Year 2000 rollover impacts, and most recently the threat of cyber terrorism. At the heart of NERC’s efforts has been a commitment to work with various federal agencies including the National Security Council (NSC), the Department of Energy (DOE), the Nuclear Regulatory Commission (NRC), and the Federal Bureau of Investigations (FBI) to reduce the vulnerability of interconnected electric systems to such threats. We hope to continue this high record of achievement by working effectively with the Office of Homeland Security.

NERC’s long history of coordination with the federal government on grid security enabled the electric industry to respond rapidly and effectively to protect the nation’s electricity production and delivery infrastructure in response to the terrible events that occurred last September. NERC maintains a close working relationship with the FBI’s National Infrastructure Protection Center (NIPC) and the Department of Energy’s Emergency Operations Center (DOE-EOC), and participates and hosts several related critical infrastructure protection programs, including the NERC Critical Infrastructure Protection Advisory Group (CIPAG); the Indications, Analysis, and Warnings Program (IAWP); the Electricity Sector Information Sharing and Analysis Center (ES-ISAC); and the Partnership for Critical Infrastructure Security (PCIS). In that same vein, NERC stands ready and able to work closely with the new Office of Homeland Security, under the leadership of Governor Tom Ridge.

In this testimony I will discuss NERC's activities on behalf of the electric industry and demonstrate that, through planning, hard work, coordination and cooperation, and effective communications, the electric industry is prepared for catastrophic events, even events as unthinkable as those that occurred on September 11, 2001. I will also discuss how information flows within the industry, and to and from industry and government. I will also discuss how the electric industry is working with the government to protect the electricity supply system against future physical and cyber attacks.

Electric Industry Response to the Terrorist Attacks of September 11, 2001

On the morning of September 11, NERC was notified that there had been apparent terrorist attacks on the World Trade Center (WTC). At about 10 a.m., NERC asked its 21 Reliability Coordinators and underlying control areas to go to "full-alert" status. Over the next several hours, NERC established contacts with the FBI, the NRC, and DOE's EOC. NERC then tested our security-related communications channels, which were operating normally. NERC communicates with its Reliability Coordinators via an Internet communications system and a private frame-relay system. We also have a secure telephone-based communications system with certain federal agencies. Throughout the day we maintained constant contact with the NERC Reliability Coordinators and continued to monitor system status across the continent. The immediate impact of the WTC attacks was the loss of electric service to lower Manhattan; approximately 400 MW of load on Consolidated Edison's system was lost. As catastrophic as this event was, it was locally contained from an electrical standpoint. The local systems worked as they were designed in accordance with local and regional reliability criteria, and at no time was the larger electric grid in any danger.

On the morning of September 12, I participated in an FBI briefing. Following that briefing and based on information received from the FBI, NERC moved its Reliability Coordinators to alert-level 2, which constitutes a heightened state of readiness but less than full alert. Since September 11, NERC has codified its alert levels in two documents: Threat Alert Levels and Physical Response Guidelines and Threat Alert Levels and Cyber Response Guidelines. Both documents were developed through a collaborative process in which all industry stakeholders participated. Today, the electric industry is at "Threatcon-low," which acknowledges the existence of a general threat of terrorist or increased criminal activity with no specific threat directed against the electric industry. The industry will remain at this level for both physical and cyber threats until NERC receives intelligence that this state of readiness is no longer appropriate.

On September 13, NERC initiated daily Reliability Coordinator calls. The FBI and EOC also participated in those calls. Those calls were in addition to the daily calls conducted by regional operators to discuss operations issues. Today, those daily calls between the ES-ISAC, NIPC and DOE-EOC continue.

On September 17, distributed denial of service (DDoS) cyber attacks started, and they continued for about a week. Several servers connected to the Internet were targeted and eventually shut down for a few hours. To my knowledge, no facilities connected with the operation of the bulk electric system, or connected with customer billing information, were

affected. On Tuesday, September 18, the now infamous NIMDA virus was unleashed. While widespread disruptions again were experienced, no electric control systems were affected.

Preparedness for Terrorism is Not New

The industry was well prepared to deal with events such as those of September 11, 2001. In 1988, NERC worked with the National Security Council, as directed by the Vice President's Task Force on Terrorism, to create a Generic Security Program, a Facility Program, and an Operations Program to combat multi-site, state-sponsored terrorism. Those activities resulted in 12 recommendations. The most important were that each operating entity must (1) have a plan that is exercised regularly in conjunction with all the other operating entities in the region, and (2) establish a contact with the local FBI office. These plans were in place and were implemented on the morning of September 11. Many of the other recommendations are also in place, such as a spare transformer database, a proper names database maintained for the FBI, changes to the operating standards to recognize sabotage and terrorism events, and an enhancement of our notification networks.

Another development in the mid-1990s that proved to be critical during the 9/11 crisis was the creation of 21 NERC Reliability Coordinators across North America. Reliability used in this context means the operation of the high-voltage transmission systems to ensure that reliability and grid integrity is maintained throughout all conceivable single contingencies. These Reliability Coordinators are responsible for seeing and understanding the big picture in terms of bulk electric system operations. They assess the moment-to-moment reliability of the grid and take actions to maintain transmission system reliability. Reliability Coordinators are authorized to call on transmission loading relief procedures or take other steps to ensure that commercial energy transactions do not overload the grid beyond NERC-established reliability criteria. These 21 Reliability Coordinators are also responsible for coordination during emergencies, and operate 24 hours-a-day, 7 days-a-week. I commend the NERC Reliability Coordinators for their extraordinary dedication and responsiveness, which was again demonstrated during the national emergency of 9/11.

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 Plan for Information Systems Protection, and to seek voluntary participation of private industry to meet common goals for protecting the country's critical systems 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, then Secretary of Energy Bill Richardson sought NERC's assistance in developing a program for protecting the nation's critical electricity sector infrastructure and NERC agreed to participate as the electricity sector coordinator.

As part of this public-private partnership, DOE, the U.S. government's designated Energy Sector Liaison worked through its Infrastructure Assurance Outreach Program to help the electric industry develop an overall security framework to address the changing industry structure and the threat of cyber and physical intrusion. The product of this effort forms the basis of NERC policy on information assurance. In addition, DOE provided clearances for a number

of industry personnel to facilitate the transfer of information to industry that may be of value in the operation of the electric systems in North America. These clearances complement those obtained from the FBI.

On at least two occasions, Congress has asked the General Accounting Office (GAO) to study the practices of organizations that successfully share sensitive information. GAO report B-247385, April 1992, "Electricity Supply, Efforts Under Way to Improve Federal Electrical Disruption Preparedness," and GAO report GAO-02-24, October 15, 2001, "Information Sharing: Practices That Can Benefit Critical Infrastructure Protection," outline and report on many of the ways in which NERC coordinates industry response activities.

Future Actions

To continue the success of the systems and programs we have in place to ensure the secure operation of the bulk electric system, NERC is examining all of our policies, standards, practices, and procedures that specifically apply to operator readiness and response to terrorism, both physical and cyber. As a result of the 9/11 attack, we have:

- asked our Compliance Enforcement Program people to quickly assess the industry's state of compliance with the standards that directly apply to terrorism.
- established a work team to identify "security risk" documents and web sites, with an eye to ensuring that critical system information does not get into the wrong hands. That team is now part of CIPAG.
- protected NERC web sites that show critical information such as real-time power flows over critical paths against those who merely may be curious, as opposed to those that rely on this information for legitimate reliability or commercial purposes.
- attained assurances from operating entities that their security plans are appropriately updated and are being routinely exercised.
- worked to ensure closer coordination between those entities responsible for physical systems and those responsible for cyber security. In the past, these activities were often addressed separately. Many electric industry organizations have reorganized to combine physical and cyber security under the same management.
- worked to reaffirm and improve our contacts with the FBI, DOE, and other government agencies.

In the longer term, we need to guarantee that NERC has the full complement of tools necessary to ensure the continued reliability of the electric grid. We need Congress to pass the reliability legislation included as part of the comprehensive energy bill recently passed by the Senate. That legislation would provide for an industry self-regulatory electric reliability organization (ERO) to set and enforce mandatory reliability rules. That matter is presently before the House-Senate Conference Committee in H.R. 4. Presently, the NERC reliability rules and the security procedures that we have in place throughout the industry are essentially

voluntary rules with no provision for enforcement. Only with mandatory enforceable standards can NERC ensure the secure and reliable operation of the bulk electric systems. NERC and most organizations representing electricity consumers, states, and utilities believe that an ERO is best situated to develop and enforce bulk power system reliability standards throughout North America. The President's National Energy Plan also endorsed the creation of an ERO, subject to Federal Energy Regulatory Commission (FERC) oversight in the U.S.

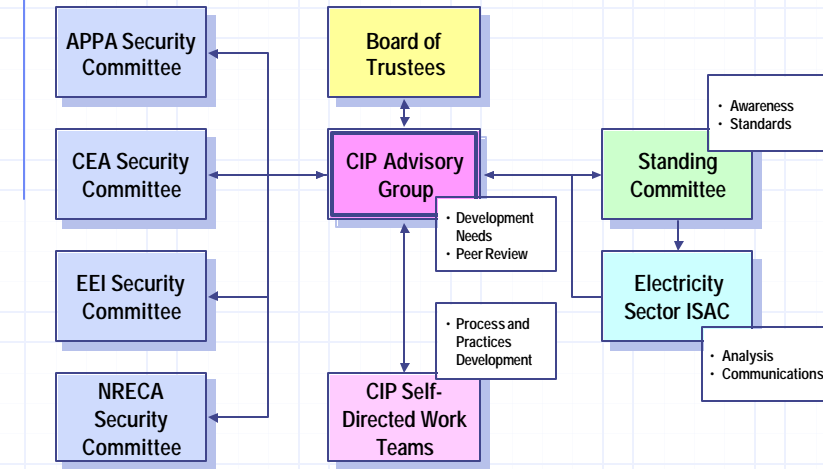
In the months ahead, our industry-based CIPAG will continue to work with government to better ensure the security of our nation's critical infrastructures. This means working closely with the new Office of Homeland Security. I personally believe that a Y2k-type of approach will be the most effective way to get the commitment of the 3,600 entities that together operate the electric grids in the United States and Canada to deal effectively with all aspects of physical and cyber terrorism. The efforts put forth by our industry in response to the Y2k threat demonstrated unmatched and unprecedented cooperation within the industry and with government. Those activities provide a strong model upon which any new infrastructure protection actions should be based.

Critical Infrastructure Protection Advisory Group

NERC created CIPAG to evaluate sharing cyber and physical incident data affecting the bulk electric systems in North America. This Advisory Group, which reports to NERC's Board of Trustees, has Regional Reliability Council and industry sector representation as well as participation by the Critical Infrastructure Assurance Office in the Department of Commerce (CIAO), DOE, NIPC, and FERC.

It is essential that all Electricity Sector segments be represented in the Critical Infrastructure Protection (CIP) development process. The participants include the dedicated experts in the Electricity Sector who represent physical, cyber, and operations security. NERC is recognized as the most representative organization of the Electricity Sector for this coordination function, as demonstrated by NERC's performance as project coordinator for the Electricity Sector for the Y2k transition. The security committees and communities associated with industry organizations (American Public Power Association, Canadian Electricity Association, Edison Electric Institute, and National Rural Electric Cooperative Association) provide the expertise for physical security in the Electricity Sector to compliment NERC's existing operational and cyber security expertise. The Advisory Group relies on small self-directed working teams, a proven and effective method for developing detailed processes and practices by subject matter experts, concluding with peer review in the forum environment.

CIP Advisory Group



Activities

CIPAG activities are conducted so as to reduce the vulnerability of the North American bulk electric system to the effects of physical and cyber terrorism. The Advisory Group's activities include developing recommendations and practices related to monitoring, detection, protection, restoration, training, and exercises.

Specific activities include:

- Identifying and coordinating with groups responsible for both physical and cyber security in all Electricity Sector segments. The organizations include APPA, CEA, EEI, ELCON, EPRI, EPSA, and NRECA.
- Provide oversight and assistance to NERC in its DOE-designated responsibility as the Electric Power Sector Coordinator, and provide liaison with government agencies.
- Recommending to the NERC standing committees on any needed modifications to NERC reliability standards dealing with emergency operations, disturbance reporting, and other CIP-related issues.
- Developing procedures for data exchange with government agencies.
- Providing oversight to the ES-ISAC.
- Maintaining the Indications, Analysis, and Warnings Program with NIPC.

- Maintaining the Electricity Sector’s Security Alert Levels.
- Providing oversight and support to the Electricity Sector’s representative on the PCIS.

Security Guidelines for the Electricity Sector

NERC’s Approach to Action defines the need to address security. Last October, CIPAG began to compile “best practices” that electricity sector entities could consider when developing and implementing their security plans. The effort resulted in a document titled *Security Guidelines for the Electricity Sector*, which is pending approval of NERC’s Board of Trustees.

The guidelines describe general approaches, considerations, practices, and planning philosophies in the following subject areas:

1. Vulnerability and Risk Assessment
2. Threat Response Capability
3. Emergency Management
4. Continuity of Business Processes
5. Communications
6. Physical Security
7. Information Technology/Cyber Security
8. Employment Screening

Recognizing that specific programs or implementation of security considerations must reflect an individual organization’s assessment of its own needs, vulnerabilities and consequences, and its tolerance for risk, the guidelines offer specific activities that may be undertaken in each of the subject areas.

National Infrastructure Protection Center Activities

NERC has a close working relationship with NIPC. The electric industry has worked closely with NIPC for about two years to develop a voluntary, industry-wide physical and cyber security indications, analysis, and warning reporting procedure. This program provides NIPC with information that, when combined with other intelligence available to it, allows NIPC to provide the electric industry with timely, accurate, and actionable alerts and warnings of imminent or emerging physical or cyber attacks. A high degree of cooperation with NIPC is possible because of the industry’s long history of working with local, state, and federal government agencies. In the late 1980s, the NERC Board of Trustees directed the NERC staff to establish and maintain a working relationship with the FBI at the national level. The Board also resolved that each electric utility should develop a close working relationship with its local FBI office, if it did not already have such a relationship. The existence of these relationships was a critical element in ensuring the industry’s coordinated and effective response to the terrorist attacks of September 11.

Indications, Analysis, and Warnings Program

One of CIPAG's first tasks was to develop the incident data types and event thresholds to be used in an information-sharing program with NIPC. Information sharing (electronic and telephone) mechanisms have been developed for use by electric transmission providers, generation providers, and other industry entities for reporting on a voluntary basis to both NIPC and NERC. Assessments, advisories, and alerts prepared by NIPC (with NERC's support), based on the data provided by the electric and other industry sectors and government sources, will be stated in an actionable manner and will be transmitted to electric industry entities. This process was tested successfully within one Regional Reliability Council during the fall and winter of 1999/2000. Because some of the analyses involve classified information, U.S. government security clearances have been obtained by key industry personnel and NERC staff members. Other electric industry personnel are in the process of obtaining security clearances. It would be useful for Congress to provide a way for sponsoring agencies, such as the FBI and DOE, to increase the number of industry personnel with security clearances.

The Indications, Analysis, and Warnings Program (IAWP), which evolved from this work, was implemented in July 2000; initial emphasis is on reporting by NERC Reliability Coordinators and utility control areas. Individual electric utilities, marketers, and other electricity supply and delivery entities are encouraged to participate by submitting incident data and receiving the various types of NIPC warnings and related materials. Workshops have been conducted to provide program details to the industry, and a more comprehensive communications program is being developed by CIPAG to encourage broader industry participation in the program. The IAWP is a key voluntary first step toward preparing the electricity sector to meet PDD-63 objectives.

Electricity Sector Information Sharing and Analysis Center

The President's Commission on Critical Infrastructure Protection recommended that each of the critical infrastructure sectors establish an Information Sharing and Analysis Center (ISAC) to help protect the infrastructures from disruption arising from coordinated intrusion or attack. The ISACs gather incident data from within their respective sectors, perform analysis to determine potential malicious intent, share findings with other ISACs (private and government) in a manner that ensures, as required, target identity protection, and disseminate actionable warnings so appropriate action can be taken within each sector. ISACs serve as points of contact between sectors to facilitate communications, especially during a time of stress. ISACs study cross-sector interdependencies to better understand and be prepared for the possible impacts of an "outage" in one sector or another.

NERC is the Electricity Sector ISAC that performs essentially the same functions that have been required of NERC for physical sabotage and terrorism. The ES-ISAC's duties are:

1. Receive voluntarily supplied incident data from electric industry entities.
2. Work with NIPC during its analysis of incident data to determine threat trends and vulnerabilities.

3. Assist the NIPC personnel during its analyses on a cross-private and federal sector basis.
4. Disseminate threat and vulnerability assessments, advisories, and alerts and other related materials to all those within the electric industry who wish to participate.

The ES-ISAC is staffed on workdays with on-call provision for all other periods. Should this capability need to be enhanced, NERC will request support for a 24-hour, seven-days-a-week staffed facility. NERC has established relationships with the other ISACs through the PCIS (see below) and will establish relationships with other ISACs as they form.

Information sharing of sensitive information among operating entities and with the ES-ISAC is seriously limited by the unavailability of communications equipment that would allow secure voice conversations. Secure communications is limited to encrypted e-mail.

Critical Infrastructure Protection Planning

The CIPAG, working with CIAO, has written a Business Case for Action to delineate the need for critical infrastructure protection by the electric industry. Separate business cases as well as a general overview have been prepared for chief executive officers, chief operating officers, and chief information officers. The purpose of the business case is to persuade industry participants to report incidents and to be mindful of the possible business losses caused by cyber and physical intrusion.

The CIPAG has developed a basic and fairly comprehensive plan to address CIP. The prototype plan, still undergoing industry review, addresses awareness, threat and vulnerability assessment, practices that can be considered, risk management schema, restoration, and interdependencies between and among sectors.

The essence of this “Approach to Action” is being considered for inclusion in Version 2.0 of the National Plan for Information Systems Protection being compiled by the U.S. Government.

Several documents related to critical infrastructure protection can be found at <http://www.nerc.com/~filez/cip.html>.

Partnership for Critical Infrastructure Security

The PCIS was established to promote public/private cooperation and communication. It is supported by CIAO and the U.S. Chamber of Commerce. In 2001, PCIS was established as a not-for-profit organization and elected a Board of Directors and company officers. NERC participates in PCIS and I serve as its Secretary. Its stated mission is to coordinate cross-sector initiatives and complement public/private efforts to promote and assure reliable provision of critical infrastructure services in the face of emerging risks to the economy and the nation’s critical infrastructure.

PCIS is focusing its efforts on these functional areas:

- National Strategy for Critical Infrastructure Assurance
- Digital Control Systems Security R&D Clearinghouse
- Effective Practices Compendium
- Critical Infrastructure Assurance Awareness Materials and Support
- Risk Assessment Guidebook
- Cross-Sector Information Exchange

Through these activities we will gain a clearer understanding of sector interdependencies, better communication between sectors via ISACs and with public stakeholders, increased sharing of common research and development efforts, and ultimately coordinated efforts to protect our nation.

Improvements to Information Sharing

As positive and useful as these activities have been, however, there is yet more information that could be provided to the government in order to assist it in helping the private sector understand such complicated potential vulnerabilities as the interdependencies between and among different infrastructures, such as telecommunications, electricity, transportation, and natural gas.

Problems Associated With Information Sharing

Any information-sharing activity, however, voluntary or not, raises serious security concerns. In particular, any time that the government has access to what is, in essence, “targeting” information, there is the risk that some hostile agent could also gain access to it and use it to do great harm. The problem becomes even more acute when information is not only required to be made available, but is then published on the internet in real time, providing easy access to anyone looking to identify weak links in the utility grid. Of course, legitimate market participants and regulators need to obtain information in a timely manner, but access to truly sensitive information must be strictly controlled.

A corollary problem exists regarding whether and how to create a structure and process for the industry to work together in order to share information and analysis, and to plan for resisting, responding to, and recovering from hostile activity. I am not an expert on the Freedom of Information Act (FOIA) or antitrust law (or even a lawyer), but I have many years of practical experience in this industry. Based on that experience, I understand that company executives and managers believe they cannot prudently discuss certain matters with their competitors, suppliers, or customers. They believe that such discussions, and especially any resulting plans or actions, could be the source of antitrust litigation. In addition, even if the company might ultimately prevail, the great expense, potential risk of adverse publicity or even temporary loss, and possible public release of sensitive information during the course of such litigation lead them to not even begin the conversation in the first place. That diminishes our ability to improve our security in advance of a problem.

These concerns go beyond the potential antitrust problems caused by merely sharing information about threats. In particular, entire industries are now having to address whether and how to share spare parts or other resources to repair major, widespread damage and prevent worse calamities due to cascading failures. The issue of sharing also involves potential allocations of scarce commodities — both supplies for repair, and products for customers. Further, entire industries may determine security-related requirements to ask of their suppliers and business partners. At the least, entire industries may discuss the security-related shortcomings of existing products, suppliers and partners. Each of these actions is ripe for allegations of illegal market manipulation (boycotts, market allocations, etc.).

These issues are not simply theoretical. DOE and OHS have asked the electric utility industry to provide the government with a list of nationally critical electric facilities. We can imagine several reasons why various agencies and levels of government each might have their own needs to be aware of the industry's most critical facilities. Certainly, the industry has been expanding its critical facilities database for its own management purposes over the last several months. However, we cannot simply ignore the security concerns we have been voicing since the mid-1980s and hand over even a small part of any such database without adequate assurance that such information will receive appropriate protection. Neither is it clear that a bare list created for the federal government's purposes would contain the same information as an industry-created list, or would have any benefit at all to the industry.

What Government Can Do to Encourage Information-Sharing

We are asking federal regulators, agencies, and states to reconsider what information they request of utilities, especially market information identifying system constraints and the availability of critical facilities. Our industry has especially asked that they reconsider how they share that information once they obtain it. In fact, the Federal Energy Regulatory Commission (FERC) is beginning to address those issues. FERC recently asked for advice and suggestions on how to prevent sensitive information from being disclosed despite the requirements of FOIA. However, there is no clear process or timeline for any final decision by FERC.

Congress is in the best position to mitigate the security risks inherent in information-sharing activities, whether voluntary or required. As to voluntary information-sharing, Senators Robert Bennett (R-UT) and Jon Kyl (R-AZ) have introduced legislation, S. 1456, that would promote voluntary information sharing about sensitive security issues among infrastructure companies, and between those companies and the government by providing limited, specific clarifications of the Freedom of Information Act (FOIA) and of federal antitrust laws for certain critical infrastructure protection information sharing efforts by the private sector. I have been informed that this proposal builds on existing relevant legal precedents such as the 1998 Y2K Information and Readiness Disclosure Act, the 1984 National Cooperative Research Act, certain (territorially limited) court rulings, as well as a very few, case-specific Department of Justice advisory letters.

Similar, bipartisan legislation, H.R. 2435, has already been introduced in the House by Representatives Tom Davis (R-VA) and James Moran (D-VA). Our industry is part of a coalition of critical infrastructure industries that strongly supports the efforts to combine these

two proposals, and we urge Congress to promptly enact the product of those efforts. The proposed legislation would be a clear statement from the government that such information-sharing organizations and activities are not only permissible, but are actively encouraged. Congress can also help mitigate security risks by providing similar direction to federal agencies and the states regarding Federal and state requirements for reporting and public dissemination of critical, sensitive data, especially information identifying system constraints and the availability of critical facilities.

Conclusion

In conclusion I would like to make three points:

- The physical properties of the interconnected electric grids require close coordination and adherence by operating entities and users of these grids to the common reliability rules. Our 34-year history of cooperation and coordination has served the industry, the United States, and Canada well. As a result, I believe the electric industry is the best prepared of all the infrastructure industries.
- Coordination and cooperation among all electric industry participants and coordination with government agencies through the Regional Reliability Council concept has been the key to this success.
- The Critical Infrastructure Protection Advisory Group plays the central role in coordinating electric industry actions to promote critical infrastructure protection.