

**TESTIMONY OF**  
**LYNN P. COSTANTINI**  
**DIRECTOR <sup>3</sup>/<sub>4</sub> INFORMATION TECHNOLOGY**  
**NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL**

**BEFORE THE**  
**SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS**  
**COMMITTEE ON ENERGY AND COMMERCE**  
**UNITED STATES HOUSE OF REPRESENTATIVES**

**July 9, 2002**

## ***Critical Infrastructure Protection: The Need for Public-Private Partnership***

### **Summary**

- The North American Electric Reliability Council (NERC) supports the Administration's proposed Department of Homeland Security.
- NERC believes it is imperative to national security to refine and strengthen the public-private partnership.
- Barriers exist that prevent the flow of information between and among the public and private sectors. However, that flow of information is crucial to protecting our critical infrastructures. We can overcome these barriers by:
  - ▶ Clarifying Freedom of Information Act (FOIA) exemptions to provide indisputable, consistent rules for the non-disclosure of critical infrastructure protection. Alternatively, create new statutes stipulating non-disclosure of specific, sensitive data provided to the United States government for the purposes of critical infrastructure protection.
  - ▶ Granting security clearances for personnel in critical infrastructure industries so that the flow of information between the public and private sectors can remain intact and secure.
  - ▶ Providing limited anti-trust exemptions such as those that enabled cross-sector coordination during the Year 2000 rollover.
  - ▶ Continuing to build trust.
- Organizing the authority and responsibilities for protecting our critical infrastructures under the Department of Homeland Security will help overcome these obstacles to protecting our critical infrastructures.

## ***Critical Infrastructure Protection: The Need for Public-Private Partnership***

My name is Lynn Costantini, and I am the Director of Information Technology for 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 of the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

In addition to its job of “keeping the lights on,” NERC serves as the electric industry’s contact and coordinator in the United States and Canada for bulk electric system security matters and operates the Electricity Sector’s Information Sharing and Analysis Center (ES-ISAC).

As the Director of Information Technology, it is my responsibility to ensure NERC’s information assets and the environment in which they operate are secure. I serve on NERC’s Critical Infrastructure Protection Advisory Group and I am a member of the ES-ISAC team.

Generally NERC supports the Administration’s proposed Department of Homeland Security. NERC appreciates the recognition in this proposal of the role of the private sector in protecting critical infrastructures. Furthermore, NERC believes it is imperative to national security to refine and strengthen the public-private partnership. Organizing the authority and responsibilities for critical infrastructure protection under the Department of Homeland Security supports that goal.

In this testimony, I will discuss the need to keep information flowing between the public and private sectors, the barriers to information sharing, what can be done to overcome those barriers, and, finally, the electricity sector’s experience in these areas.

### **Background**

The information age dawned with little thought to security. We were in awe of the power at our fingertips (information!) and we rushed to find new ways to gather and use more and more information through an increasing array of new techniques. A computer on every desktop, complete with tools to improve efficiency and productivity, networked together so we could share precious resources. How could something so positive, so beneficial, be used against us? Never!

Today we know better. The silver cloud had a black lining. First “script kiddies” exploited vulnerabilities in our computing armor for fun. Then committed hackers exploited us for profit. Now we are faced with the prospect of nation-states exploiting us to rain terror. The need for security was never clearer or more urgent.

We now also understand that security is multi-faceted. It is guards, gates, and guns. It is firewalls and intrusion detection systems. It is policy statements and disaster planning. It is also about understanding the spectrum of threats we face so we can accurately assess risk in the

context of our industries, our operating environments. Ultimately, security is about awareness, preparedness, and action.

### **The Need for Partnership**

Security, then, demands cooperation and coordination between the public and private sectors. In fact, the public-private relationship is vital. It is true that more than 80% of assets that drive our economy are privately held. However, without the assistance of the United States government to help the owners of these assets understand their threat environment and warn them when they are called out as targets, these assets may be vulnerable.

Moreover, the public-private partnership is crucial to helping us understand such complicated potential vulnerabilities as the interdependencies between and among different infrastructures, such as telecommunications, electricity, transportation, and natural gas.

### **Barriers to Public-Private Partnership**

Although the idea of information sharing seems so simple, it raises serious concerns. Except in special circumstances, information provided to the government is subject to disclosure to the citizenry and others via the Freedom of Information Act (FOIA). Furthermore, information sharing among members of private industry is subject to anti-trust regulations. Trust is as much an issue as anti-trust.

### **Freedom of Information Act**

Participants in critical infrastructure industries repeatedly cite the inability of the federal government to assure them that any sensitive information they supply will not fall into inappropriate hands as a significant barrier to information flow between the public and private sectors. The effect of these private-sector concerns is that some valuable information necessary to fully analyze vulnerabilities and risks to critical national interests is not being reported. This will likely remain the case until the government can offer such assurances of protection from disclosure.

Of course, legitimate market participants, regulators, and others need to obtain information in a timely manner, but truly sensitive information must be protected.

The existing FOIA disclosure exemptions do not provide the necessary levels of assurance.

Exemption 4 asserts that information voluntarily given to the government will be protected if the provider customarily treats such information as confidential. This language leaves the door open to legal challenges and thus, to the possibility of disclosure of sensitive information. Rather than risk disclosure, the private sector may decide not to release information to the government.

Exemption 1 protects sensitive information from disclosure by classifying it in the interest of national defense or foreign policy. This is strong, assuring language; however, only a small percentage of the personnel working in critical infrastructure industries have security clearances. The flow of information from the public sector back to the private sector would be jeopardized if sensitive information were classified.

FOIA disclosure concerns are not simply theoretical. The United States Department of Energy, working with the Office of Homeland Security, has asked the electric utility industry to provide

the government with a list of nationally critical electric facilities. We understand how this information would be useful. Indeed, NERC has maintained a critical equipment database since the mid-1980s, to which strict access controls are applied. NERC and its members are unwilling to hand over even a small part of any such database without adequate assurance that such information will receive appropriate protection.

### **Anti-trust Regulations**

Anti-trust regulation is another serious private-sector concern and goes beyond the potential problems caused by merely sharing information about threats. Entire industries must decide whether and how to share spare parts or other finite 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 anti-trust allegation. The risk of allegation seriously dampens the willingness to share information, which, in turn, jeopardizes the ability to adequately analyze cross-sector dependencies and develop effective protection strategies.

### **Trust**

As noted by the General Accounting Office last October, one issue critical “to establishing, developing, and maintaining effective information-sharing relationships [to] benefit critical infrastructure protections efforts, [is to] foster... trust and respect...”<sup>1</sup> Without a trust relationship between government and private industry, information sharing stands little chance of success.

A report by the President’s Commission on Critical Infrastructure Protection (PCCIP) in October 1997 specifically commended NERC as a model for information sharing, cooperation, and coordination between the private sector and government. Clearly, the successful relationship between NERC and its government partners — the FBI and its National Infrastructure Protection Center, the Department of Energy, and others — has been a benefit to the electricity sector.

### **Overcoming the Barriers to Public-Private Partnership**

#### **Clarify the Freedom of Information Act disclosure exemptions.**

FOIA disclosure exemptions do not provide the necessary levels of assurance to the private sector that its sensitive information will be protected. Congress should clarify the exemptions to create indisputable, consistent rules for the non-disclosure of sensitive critical infrastructure protection information. Alternatively, create new statutes stipulating non-disclosure of specific, sensitive data voluntarily provided to the United States government for the purposes of critical infrastructure protection.

Because of the FOIA concerns, participants in the electricity sector are asking federal regulators, agencies, and states to reconsider what information they request of utilities, especially market information that identifies system constraints and the availability of critical facilities. Our

---

<sup>1</sup> **Information Sharing – Practices That Can Benefit Critical Infrastructure Protection**, GAO Report to Senator R. F. Bennett, Joint Economic Committee (October 2001)

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.

**Grant security clearances for personnel in critical infrastructure industries so that the flow of information between the public and private sectors remains intact and secure.**

The owners of critical infrastructure assets need access to more specific threat information and analysis from the public sector in order to develop adequate protection strategies. This may require either more security clearances or treatment of some intelligence and threat information and analysis as sensitive business information, rather than as classified information.

**Provide limited anti-trust exemptions.**

The possibility of anti-trust allegations inhibits cross-sector information sharing. The private sector wants clarity as to what information it can share and the extent to which information can be exchanged without risking anti-trust allegations. A legislative action similar to the 1998 Y2K Information and Readiness Disclosure Act would provide the necessary level of clarity.

**Build Trust**

Infrastructure security requires a healthy, trusting public-private relationship. Overlapping and inconsistent roles and authorities may have hindered development of productive working relationships. Clarification of roles and responsibilities both within the government and the private sector is an important factor in building a trust model. Centralizing leadership, authority, and responsibility under the Department of Homeland Security is a step forward in building trust. Recognizing a voluntary system of information sharing between the public and private sector as an effective means of promoting critical infrastructure assurance is another. Helping the private sector overcome barriers to effective participation by clarifying FOIA and providing anti-trust protection will allow the trust relationship to grow and be fruitful.

**The Electricity Sector Experience**

NERC has a long history of coordination with the federal government on grid security. It 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 physical and 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.

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 in and hosts several related critical infrastructure protection programs, 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).

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.

**Information Sharing and Analysis Center for the Electricity Sector (ES-ISAC)**

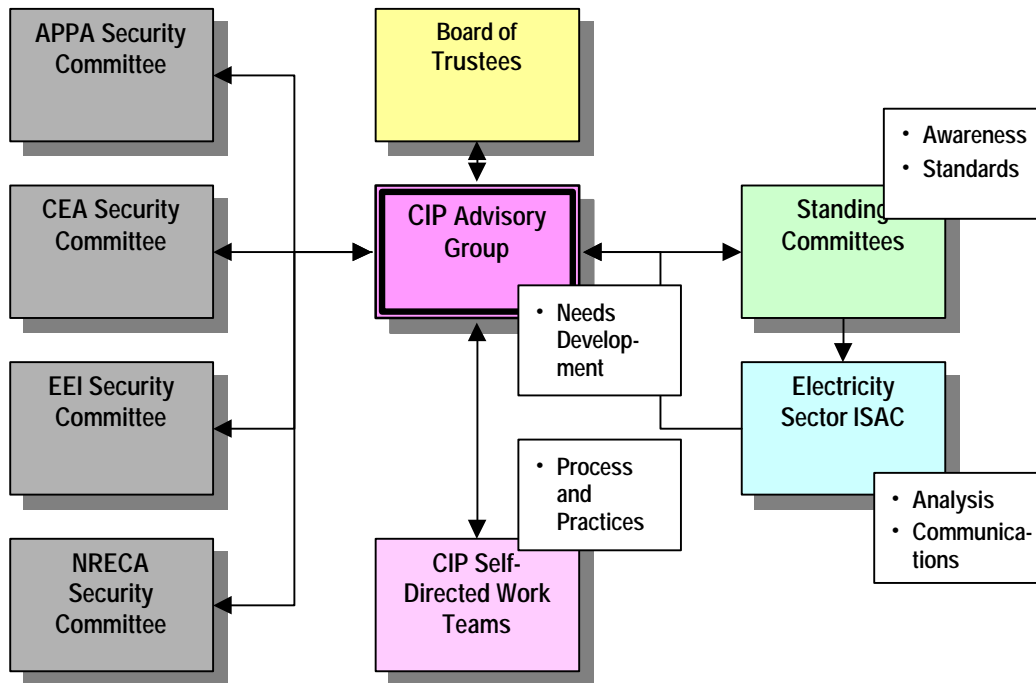
Presidential Decision Directive (PDD-63), issued in May 1998, called for government agencies to become involved in the process of developing a National Plan for Information Systems Protection, and to seek voluntary participation of private industry to meet common goals for protecting the country's critical systems through public-private partnerships. In September 1998, then Secretary of Energy 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.

In its role as the ES-ISAC, NERC performs the following functions:

- Receives incident data from electricity sector entities
- Assists the National Infrastructure Protection Center to analyze electricity sector events
- Disseminates threat and vulnerability assessments
- Liaisons with other ISACs
- Analyzes sector interdependencies
- Participates in infrastructure exercises

**Critical Infrastructure Protection Advisory Group**

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



Participation in CIPAG represents all electricity sector segments, which is an essential ingredient to its success. 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 security in the electricity sector to compliment NERC's existing operational and cyber security expertise. The CIPAG 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, and approval by NERC's Board of Trustees.

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

### Conclusions

NERC believes it is imperative to national security to refine and strengthen the public-private partnership. Building a strong trust relationship is essential to the success of this partnership. Overcoming the hurdles to effective communications and information sharing as described in this testimony will enable cooperation for the ultimate goal of protecting our nation's critical infrastructures, its economy, and the well-being of all its citizens. Thank you.

**Lynn P. Costantini**  
**Director <sup>3/4</sup> Information Technology**  
**North American Electric Reliability Council**  
**(NERC)**

Ms. Costantini joined NERC in 1983. She has held a variety of positions with the organization including Director of the Generating Availability Data System. As Director of Information Technology, Ms. Costantini is responsible for ensuring NERC's information assets and the environment in which they operate are secure. She and her team also develop and maintain systems used by the electric industry to monitor system conditions in near-real time.

Ms. Costantini serves on NERC's Critical Infrastructure Protection Advisory Group and is a member of NERC's ES-ISAC operations team.

She has worked with the industry and the Department of Energy to create *Security Guidelines for the Electricity Sector* and is currently assisting the Federal Energy Regulatory Commission in a similar activity in support of deregulated energy markets.

Ms. Costantini holds a BA degree in Economics, and a Master's Degree in Business Administration.