Testimony to

The United States House of Representatives

Committee on Government Reform

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

Discussing

Activities Undertaken by the Electricity Sector to Address Physical and Cyber Security with Emphasis on the Electricity Sector – Information Sharing and Analysis Center (ES-ISAC)

Prepared by
Louis G. Leffler, Manager-Projects
North American Electric Reliability Council

July 24, 2002

Activities Undertaken by the Electricity Sector to Address Physical and Cyber Security with Emphasis on the Electricity Sector – Information Sharing and Analysis Center (ES-ISAC)

Thank you for the opportunity to present to the Subcommittee's oversight hearing on Cyber Terrorism and Critical Infrastructure Protection some of the concepts being established by the Electricity Sector to enhance the security of our Nation's critical infrastructures.

My name is Lou Leffler. I am Manager-Projects 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).

In my role, I have the responsibility to facilitate the work of NERC's Critical Infrastructure Protection Advisory Group; I am a member of the ES-ISAC team, and Sector Coordinator.

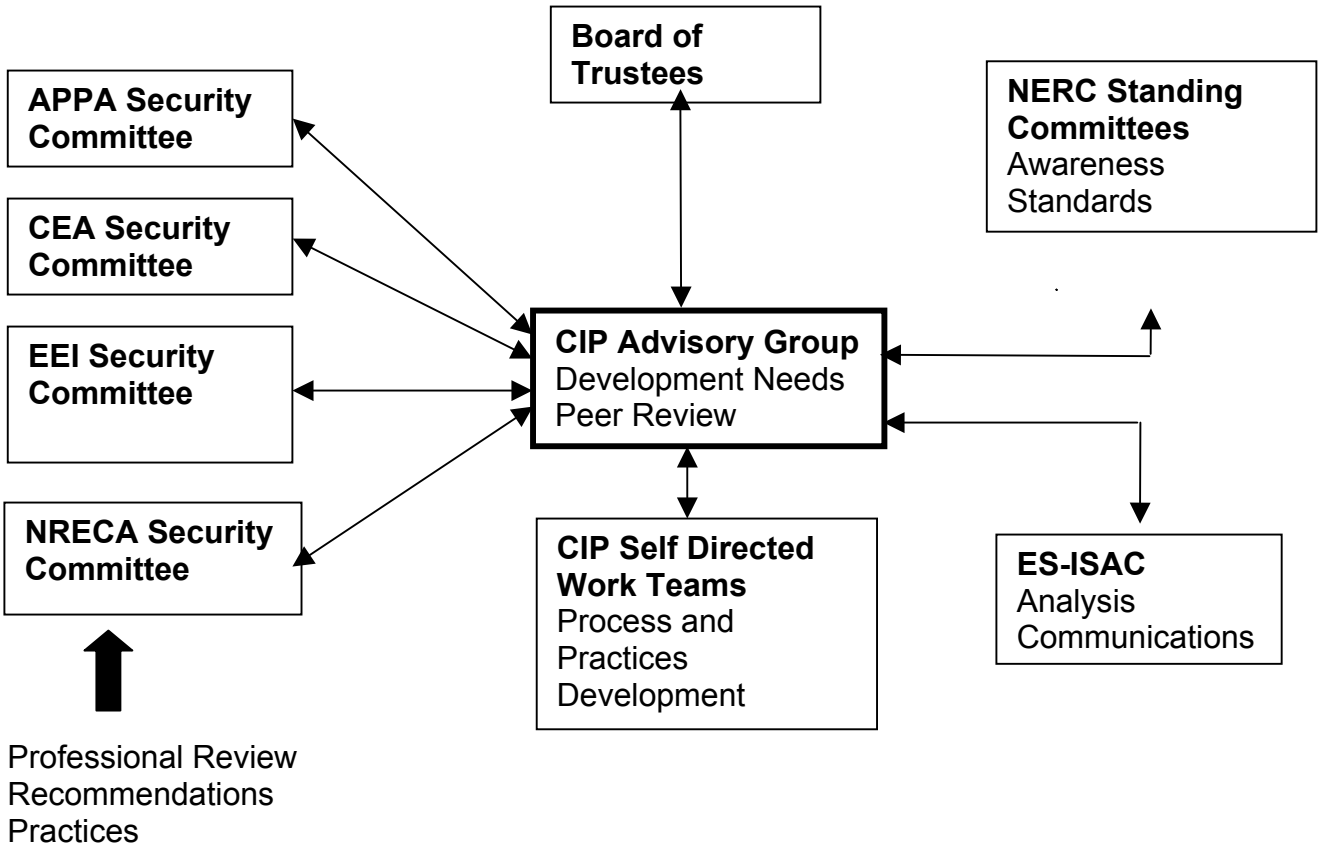
We have been requested to provide a description of the security actions taken by the Electricity Sector with primary emphasis in this testimony focused on the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

Before delving into ISAC and related matters, let me state that NERC supports the National Strategy for Homeland Security presented by the President last week. Some legislative recommendations are discussed herein.

Organization

Following issuance of the President's Commission on Critical Infrastructure Protection in 1997 and the President's Decision Directive 63 in 1998, the Secretary of the U.S. Department of Energy requested NERC to accept the role as Electricity Sector Coordinator (for Critical Infrastructure Protection). NERC President and CEO, Michehl Gent, with approval of our Board of Trustees, accepted this assignment as a logical extension of NERC's mission. NERC established a study and action group — which is now the Electricity Sector Critical Infrastructure Protection Advisory Group (CIPAG) with a direct reporting relationship to the NERC Board. Essential to progress in our efforts to enhance security of the Electricity Sector is the cooperation of all segments within the Sector. The CIPAG brings together the generation and transmission providers, public and investor-owned utilities, power marketers, regional transmission organizations and independent system operators, electric power associations, and government agencies. Both Canadian and United States entities participate.

The CIPAG is organized as depicted below.



APPA	American Public Power Association
CEA	Canadian Electricity Association
EEI	Edison Electric Institute
NRECA	National Rural Electric Cooperative Association

Indications, Analysis, and Warning Program

After the CIPAG established its relationship with our Sector Liaison, the U.S. Department of Energy (DOE), the advisory group and representatives of the DOE met with the National Infrastructure Protection Center (NIPC). From this has emerged a close security working relationship that resulted in the development of the Electricity Sector – NIPC Indications, Analysis, and Warning Program (IAW Program).

(From the IAW Program):

> This SOP (Standard Operating Procedure) establishes voluntary procedures for implementing the information reporting, analysis and warning provisions of the National Infrastructure Protection Center's (NIPC) national level Indications, Analysis & Warning (IAW) program for electric power. This program has been established to enable the NIPC to provide timely, accurate, and actionable warning for both operational and cyber threats or attacks on the national electric power infrastructure.

The IAW Program provides several reporting mechanisms to enable reliable and secure communications between Electricity Sector entities and the NIPC. The IAW Program SOP contains event criteria and thresholds with report timing for nine physical/operational and six cyber/social engineering "event types." Those events to be reported include those occurrences to an Electricity Sector entity that are either of known malicious intent or are of unknown origin. Events include such things as the loss of a key element of an electric power system or telecommunications critical to system operations, announced threats, intelligence gathering (surveillance), computer system intrusion (each event type contains specificity as to level of actual or potential impact on operations of the reporting electric entity). Note

that electric "entities" include generation, transmission, distribution, overall system reliability coordination, power marketing.

The power of the IAW Program lies in the fusion of incident information from many sources (government and private sectors) in one place for continuous analysis and prompt dissemination of threat and possible vulnerability information back to the sectors.

The IAW Program was approved for voluntary use by the Electricity Sector in July 2000. Over the next several months, NERC and NIPC conducted three workshops designed to raise the Sector's awareness to the security issues and to introduce the IAW Program. The program is in use currently.

Electricity Sector — Information Sharing and Analysis Center (ES-ISAC)®

The ES-ISAC was formed to:

- Obtain security information related to possible threats or suspicious activity, or actual malicious or terrorist acts against the Electricity Sector and to assure that this information is provided to the NIPC for analysis.
- Assist the NIPC in its analysis of the actual or potential impact of threat to or vulnerabilities of the Electricity Sector. Subject matter expertise may be provided directly by ISAC personnel or through contact with Sector people arranged via the ISAC.
- Immediately disseminate threat and vulnerability warnings on a Sector, geographic, facility type, specific facility basis as appropriate.
- Provide ongoing Sector awareness to the ever-changing security landscape.

With Board approval, NERC announced the ES-ISAC in October 2000. This function has grown in capability and support since then. It is staffed by NERC personnel who consult with particular subject

matter experts throughout the Sector. The CIPAG provides functional oversight to the ES-ISAC with regular review at each meeting.

The ES-ISAC Mission

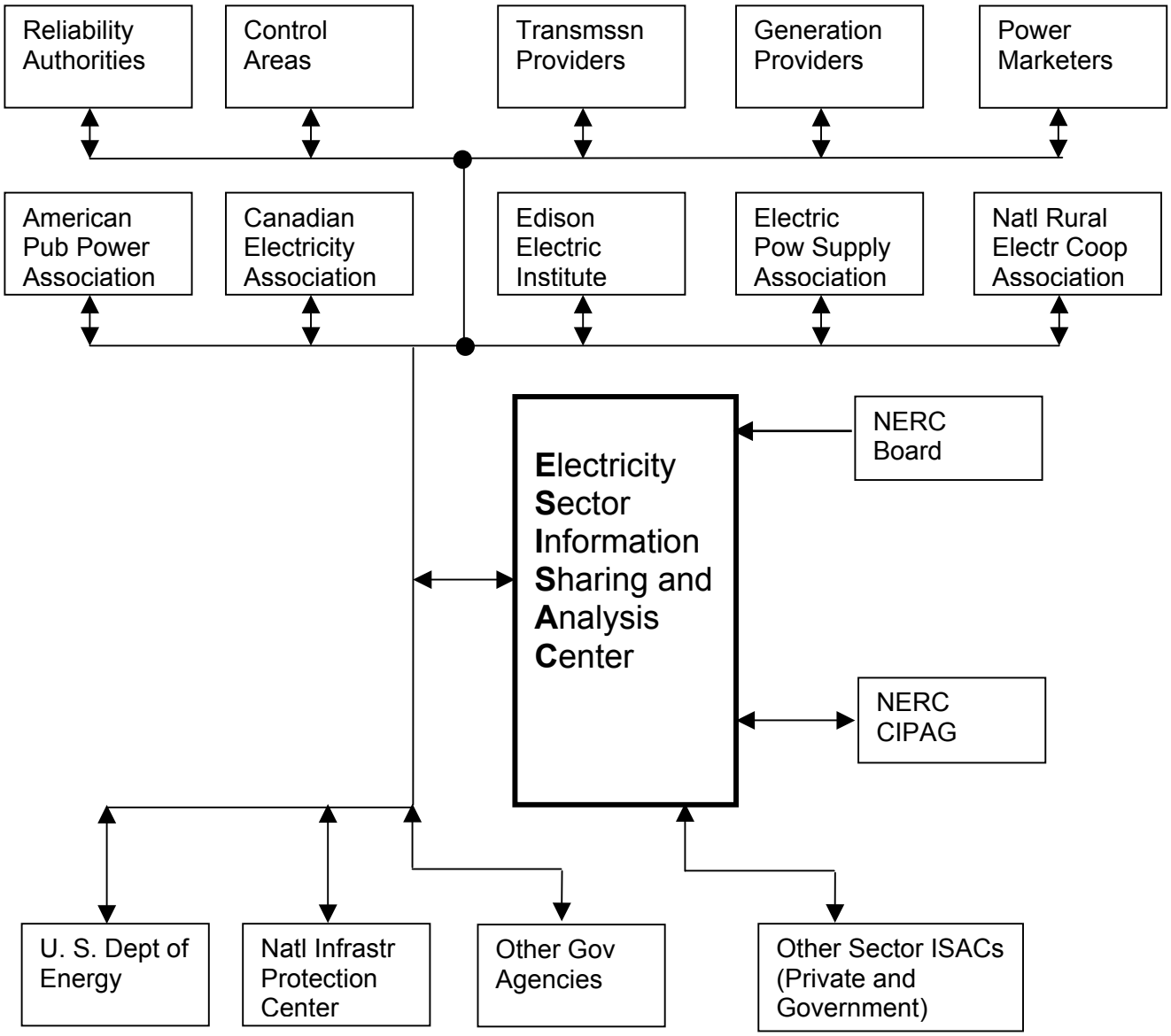
- Receive Electricity Sector information for analysis by government agencies and the ISAC.
- Provide analytical support to the NIPC and other government agencies in the interpretation of information relevant to the Electricity Sector.
- Promptly disseminate threat indications, analyses, warnings together with interpretations to assist the Electricity Sector in taking protective actions.

ES-ISAC Objectives

- As Electricity Sector Coordinator work closely with the U.S. Department of Energy (Sector Liaison) and the Canadian Office of Critical Infrastructure Protection and Emergency Preparedness.
- Assist the National Infrastructure Protection Center (NIPC) in incident analyses.
- Receive incident data from all ES entities.
- Disseminate threat and vulnerability assessments to ES entities.
- Liaison with other government and private ISACs.
- Analyze Sector interdependencies.
- Participate in infrastructure exercises.

The ES-ISAC Organization is depicted below.

ELECTRICITY SECTOR INFORMATION SHARING AND ANALYSIS CENTER



(All data and information streams depicted above are voluntary.)

A Few ES-ISAC Particulars

- There are currently seven NERC employees detailed to the ES-ISAC. The actual amount of time spent on ES-ISAC duties by each individual varies.

- The ES-ISAC has established multiple communications including telephone, secure telephone (STU-3), fax, satellite phone, pagers, secure messaging system, e-mail listservers, Internet site. The ES-ISAC is not currently staffed 24x7; staff is on 24x7 call.

- The ES-ISAC and the CIPAG coordinate with many organizations, including:

  - American Gas Association
  - American Petroleum Institute
  - American Public Power Association
  - Canadian Electricity Association
  - Critical Infrastructure Assurance Office
  - Department of Defense
  - Department of Energy and several National Laboratories
  - Department of the Interior
  - Edison Electric Institute
  - Electric Power Supply Association
  - Electricity Consumers Council
  - Federal Energy Regulatory Commission
  - National Infrastructure Protection Center
  - National Rural Electric Cooperative Association
  - Nuclear Energy Institute
  - Nuclear Regulatory Commission
  - Oil and Gas Sector
  - Partnership for Critical Infrastructure Security
  - Rural Utility Services

- The ES-ISAC is funded as part of the NERC budget which is approved by the independent Board of Trustees. There are no fees to those participating Electricity Sector entities.

Other Security-Related Activities

Following are other activities undertaken by NERC:

- Published an Approach to Action for the Electricity Sector

- Published Security Cases for Action for the Electricity Sector

- Developed a set of Security Guidelines:

  - Executive Summary
  - Communications
  - Emergency Plans
  - Employee Background Checks
  - Physical Security
  - Threat Response
  - Vulnerability Assessments
  - Continuity of Business Practices
  - Cyber Security: Access Controls
  - Cyber Security: Firewalls
  - Cyber Security: Intrusion Detection Systems
  - Cyber Security: Risk Management
  - Protecting Potentially Sensitive Information

- Developed Threat Alert Levels

  - Physical
  - Cyber

The above documents are available via the NERC and ES-ISAC Internet sites:

- <http://www.nerc.com>

- <http://www.esisac.com> (under development)

What Government Can Do to Encourage Information Sharing

The more information that is shared among and between government agencies and ISACs, the better will be each of the ISAC's ability to respond to the threats we may face and vulnerabilities we may have. But this raises concerns about the consequences of unauthorized public disclosure of highly sensitive information. Specific areas for policy consideration follow.

- 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 critical infrastructure entities, and between those entities 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.

- We recommend revisions to the Freedom of Information Act to permit more sharing of certain information with the government that may be critical to analysis, but not of general need by the public. We understand that the Committee on Government Reform has recommended including FOIA relief as part of the Homeland Security Bill, and we thank the Committee.

- We have concern for the ease of access to sensitive and perhaps vulnerability revealing electricity system information. We fully recognize the need to provide electric power system information to those operating, overseeing, regulating, or otherwise managing the power system, and we recommend more definition of the relevant access.

- We recommend revisions to antitrust laws to permit more freedom to share information among Electricity Sector entities that may be critical to analysis. Because the electric industry is very tightly interconnected on a physical basis, cooperation is requisite. Now a new area of cooperation has arisen — security.

- We request more rapid response to the requests for granting U.S. government clearances to key Electricity Sector personnel to permit the capability to more fully analyze and understand the threats to the Electricity Sector and to interdependent infrastructures.

- The very essence of ISAC operations and resultant value add to any sector requires communications. We must increase the availability of reliable and secure telecommunications for use among Sector participants, the government, and the ES-ISAC.

Conclusions

In conclusion, I would like to make these points:

- The electric industry operates in a constant state of preparedness. Planning, training, and operating synchronous grids prepares the electric industry for natural disasters such as earthquakes, floods, tornados, energy emergencies — and attacks of sabotage or terrorism.

- 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 reports directly to NERC's Board of Trustees.

- NERC serves as the electric industry's contact and coordinator in the United States and Canada for bulk electric system security matters and provides the ES-ISAC.

- Coordination and cooperation among all Electricity Sector participants and with government agencies will continue to be the key to security.

We greatly appreciate our close relationship with the Department of Energy (our Sector Liaison), the National Infrastructure Protection Center (our partner in the IAW Program), the Critical Infrastructure Assurance Office, and the Federal Energy Regulatory Commission.

Thank you very much for this opportunity to present the work undertaken by the Electricity Sector with the support of several government agencies to help secure the Electricity Infrastructure of the United States and Canada.