Congressional Research Service

Report RS21958

Government Activities to Protect the Electric Grid

Amy Abel, Resources, Science, and Industry Division

February 4, 2005

Abstract. The electric utility system is vulnerable to outages caused by a range of activities, including system operator errors, weather-related damage, and terrorist attacks. The main risk from a successful terrorist attack against the electric power industry would be widespread power outages lasting for an extended period of time. While the electric utility industry has the primary responsibility for protecting its assets, federal and state government agencies also have been addressing physical security concerns. This report provides a description of initiatives within the Federal Energy Regulatory Commission and the Departments of Energy, Homeland Security, and Defense to protect the physical transmission infrastructure.

Order Code RS21958
Updated February 4, 2005

Government Activities to Protect the Electric Grid

Amy Abel
Specialist in Energy Policy
Resources, Science, and Industry Division

Summary

The electric utility system is vulnerable to outages caused by a range of activities, including system operator errors, weather-related damage, and terrorist attacks. The main risk from a successful terrorist attack against the electric power industry would be widespread power outages lasting for an extended period of time. While the electric utility industry has the primary responsibility for protecting its assets, federal and state government agencies also have been addressing physical security concerns. This report provides a description of initiatives within the Federal Energy Regulatory Commission and the Departments of Energy, Homeland Security, and Defense to protect the physical transmission infrastructure. It will be updated as events warrant.

The U.S. electric power system has historically operated at such a high level of reliability that any major outage, caused by either sabotage, weather, or operational errors, makes news headlines. The transmission system is extensive, consisting mainly of transformers, switches, transmission towers and lines, control centers, and computer controls. A spectrum of threats exists to the electric system, ranging from weather-related incidents to terrorist attacks — including physical attacks as well as attacks on computer systems, or cyber-attacks. The main risk from weather-related damage or a terrorist attack against the electric power industry is a widespread power outage that lasts for an extended period of time.

Of the transmission system's physical infrastructure, high-voltage (HV) transformers are arguably the most critical component. Utilities rarely experience loss of an individual HV transformer, but recovery from such a loss takes months if no spare is available. Conversely, utilities regularly experience damage to transmission towers due to both weather and malicious activities and are able to recover from this damage fairly rapidly. Occasional outages resulting from these attacks generally have not been widespread or long-lasting.

Overview of Government Initiatives

The electric utility industry is evolving to become more competitive at both the wholesale and retail levels. The Energy Policy Act of 1992 (EPACT) introduced wholesale competition in the electric power industry, and subsequent Federal Energy Regulatory Commission (FERC) orders have encouraged the formation of regional transmission organizations to facilitate access to the transmission system.[1] In addition, many states have moved to allow competition on the retail level. Reliability and infrastructure protection were not addressed in EPACT and state restructuring laws, and there is currently no federal regulation of electric network security.[2] Until recently, impacts of competition on physical and cybersecurity of the electric power industry were not part of the congressional debate.[3]

The potential for terrorist attacks on the electric system has pushed secure operation of the grid into the federal policy arena from its traditional position as an industry responsibility. In 1996, the President's Commission on Critical Infrastructure Protection was created to address concerns relating to the vulnerability of critical national infrastructures. The commission issued a report in October 1997 that described electric power vulnerabilities. The report stated:

> Of particular concern are the bulk power grid (consisting of generating stations, transmission lines with voltages of 100 kV or higher, plus 150 control centers and associated substations) and the distribution portion of those electric power systems where interruption could lead to a major metropolitan outage.[4]

In response to the commission's report, President Clinton signed Presidential Decision Directive 63 (PDD-63), which outlines a series of actions designed to defend critical infrastructures from various threats.[5] On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7), which supersedes portions of PDD-63 and clarifies that the Department of Energy is the lead agency with which the energy industry will coordinate responses to energy emergencies. However, it has limited authority in the infrastructure assurance area. The North American Electric Reliability Council (NERC), an industry organization that promotes the reliable operation of the

---

[1] FERC Orders 888, 889, and 2000.

[2] See CRS Report RL32728, *Electric Utility Regulatory Reform: Issues for the 109th Congress*, by Amy Abel.

[3] Testimony of Phillip G. Harris, President and CEO, PJM Interconnection, L.L.C. Hearing Before the Subcommittee on Energy and Air Quality. House Committee on Energy and Commerce. Serial No. 107-64. October 10, 2001.

[4] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures — The Report of the President's Commission on Critical Infrastructure Protection*, U.S. Government Printing Office (GPO), No. 040-000-00699-1, October 1997.

[5] See *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, White Paper, May 22, 1998, at [http://www.usdoj.gov/criminal/cybercrime/white_pr.htm]. For a discussion on general critical infrastructure activities, see CRS Report RL30153, *Critical Infrastructure: Background, Policy, and Implementation*, by John D. Moteff.

electric system, is designated by PDD-63 as the sector coordinator for the private electric utility sector. NERC retains responsibility for promulgating and overseeing reliability guidelines for the electric power industry but does not have enforcement authority. Compliance with these guidelines is voluntary for electric utilities. As was seen in the August 14, 2003, blackout, reliability guidelines were not followed, resulting in catastrophic consequences.[6]

As electric utility sector coordinator, NERC is responsible for assessing sector vulnerabilities and developing a plan for the utility sector to reduce system vulnerabilities; proposing a system for identifying and averting attacks; and developing a plan to alert, contain, and deflect an attack in progress and then to reconstitute minimum essential capabilities in the aftermath of the attack. As part of PDD-63, Information Sharing and Analysis Centers (ISACs) have been created in many critical sectors to facilitate the gathering, analyzing, and disseminating of information related to infrastructure vulnerabilities, threats, and best practices among government and private-sector organizations. NERC operates the ISAC for the electric utility industry.[7]

Prior to the creation of the Department of Homeland Security (DHS), coordination of electric infrastructure protection activities was the responsibility of the Department of Energy (DOE). Portions of DOE's energy infrastructure security and assurance activities, including parts the Office of Energy Assurance and the National Infrastructure Simulation and Analysis Center, were transferred to DHS on March 1, 2003. The Department of Energy retains responsibility for energy supply and demand issues; energy reliability; energy emergencies; technology; training and support; coordination; and energy policy. The critical infrastructure protection functions of the Department of Homeland Security are generally expected to include security issues; threats and terrorism; and critical infrastructure protection. However, according to both DOE and DHS, their responsibilities overlap on some energy security issues, including emergencies, vulnerability, and critical assets.[8] Even though DHS and DOE have various responsibilities for infrastructure protection, they have no regulatory authority to force utilities to implement security initiatives.

Critical Electricity Infrastructure Information. Many in the industry have expressed concerns that proprietary information relating to infrastructure security could be made public if the information is shared with government agencies.[9] FERC's Order 630 allows access to certain critical energy infrastructure information (CEII) that is submitted to the Commission that would otherwise be unavailable under the Freedom of

---

[6] U.S.-Canada Power System Outage Task Force, *Interim Report: Causes of the August 14th Blackout in the United States and Canada*, November 2003.

[7] See [http://www.esiac.com/].

[8] Office of Energy Assurance, Department of Energy, Presentation to the State Heating Oil and Propane Conference, August 11, 2003; and personal communication with Department of Homeland Security.

[9] Another industry concern is that sharing information among utilities may raise antitrust problems.

Information Act (FOIA).[10] The rule defines CEII as information that "must relate to critical infrastructure, be potentially useful to terrorists, and be exempt from disclosure under the Freedom of Information Act," but excludes from release "information that identifies the location of infrastructure." The rule also establishes procedures for the public to request and obtain such critical information, and applies both to proposed and existing infrastructure. In issuing its order, FERC defined critical infrastructure as

> existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters.[11]

Proponents of FERC's rules for CEII believe they will provide adequate protection for transmission owners filing security information in future rate cases and other proceedings. Some utilities remain concerned, however, that despite the CEII rules, security information filed with FERC may still end up in the public domain — so they have been reluctant to submit specific security information to the Commission.

On February 20, 2004, DHS established the Protected Critical Infrastructure Information (PCII) Program. The PCII program is designed to encourage private industry and others with knowledge about critical infrastructure to share confidential, proprietary, and business-sensitive information with the U.S. government. DHS exempts from public disclosure all information given to the PCII program.

Many government organizations and utilities maintain databases of critical infrastructure of the electric utility industry, each containing different assets but none that identifies and locates all of the nation's utility infrastructure. In addition, there is no power-flow model for the entire United States that could, in real time, assess the vulnerabilities of regions to attacks on critical assets. At issue in attempting to develop a database of critical infrastructure is to define common parameters and purposes to assess the criticality of particular utility infrastructure. Without consistent criteria for what makes a type of infrastructure critical, either on a regional or national basis, a database of assets would be of limited value. DHS has compiled a preliminary list of critical infrastructure in electric power and has circulated that list to certain infrastructure owners for their revisions. Among utilities, there is some confusion as to why certain assets were included in the list, since some assets that are listed are not currently being used and others do not support significant load.[12] In a speech on February 23, 2004, Homeland Security Secretary Ridge announced that by December 2004, DHS will create a "unified, national critical infrastructure database that will enable us to identify our greatest points of vulnerability, existing levels of security, and then add increased measures of protection

---

[10] Federal Energy Regulatory Commission. Final Rule. Critical Energy Infrastructure Information. Order No. 630. Docket Nos. RM02-4-000-000 and PL02-1-000-000. Issued February 21, 2003.

[11] 18 CFR 388.113(c)(2).

[12] Personal communication with industry official, September 29, 2003.

where needed."[13] DHS officials have shared a draft list of critical infrastructures with some Members of Congress, but an official database has not been created.

Department of Homeland Security Protective Activities. DHS has been addressing high-voltage transformer security within its Protective Security Division (PSD) but currently is not addressing transmission towers or control center security. PSD is developing a National Emergency Energy Spare Parts Program to "ensure a supply and support system to provide spares for the critical components in our nation's infrastructure."[14] The program is initially focused on HV transformers, although it will include other types of electrical equipment in the future. As part of this program, PSD is building upon the Electric Power Research Institute's (EPRI's) transformer activities to develop a "containerized" HV recovery transformer that could fit in a conventional International Standards Organization (ISO)-compliant shipping container for easy transport on flatbed trucks. The division believes that such containerized HV transformers could not only serve as emergency replacements in a wide range of network applications, but could also be transported within a few days in emergencies.[15] According to PSD officials, the division plans to fund the development of these transformers to demonstrate the technology, but does not plan to buy a stockpile of production units; the division's emphasis is on attack prevention, rather than recovery.[16] PSD expects designs for the containerized transformers to be completed by the end of 2004.

According to PSD, the division intends to develop and implement "buffer zone" protection plans for critical power facilities, including HV transformer substations. These plans would seek to enhance security immediately around a critical facility with measures such as road barriers and surveillance to deter or delay terrorist attacks. According to PSD, local law enforcement agencies would be eligible for funding from DHS grants to states to support these buffer zone plans. PSD does not intend to evaluate or enforce transmission owners' internal security programs for critical assets. DHS is also developing grid monitoring capability.[17] More detailed information is not available from DHS.

Department of Defense. The Department of Defense Infrastructure and Interdependency Solutions Branch is developing an extensive modeling capability for many critical infrastructures, including for the electric utility industry. When complete, the model will include a map of facility locations (power plants, power lines and substations). This is intended to allow for identification of key links and nodes critical to the delivery of electric power to points or regions of interest. According to the branch

---

[13] Secretary Tom Ridge. Speech on the One-Year Anniversary of the Department of Homeland Security. George Washington University, Homeland Security Policy Institute, Washington, D.C. February 23, 2004.

[14] Department of Homeland Security (DHS), IAIP Protective Security Division. "National Emergency Energy Spare Parts Program." Presentation to the EPRI Infrastructure Security Initiative Meeting. Palo Alto, CA. June 26, 2003.

[15] DHS, June 26, 2003.

[16] DHS, personal communication, October 23, 2003.

[17] Department of Homeland Security, IAIP Protective Security Division. Personal communication. November 5, 2003.

head, the facilities on the map will then be indexed to an operational model of the power grid and a powerflow analysis tool that will allow for the identification of key links and nodes for the entire United States.[18]

Department of Energy. The Office of Energy Assurance (OEA) in the Department of Energy has lead responsibility for the security of U.S. energy infrastructure, broadly, under Homeland Security Presidential Directive 7. The OEA has expressed concern about system vulnerabilities and has been meeting informally with utility and transformer industry representatives to explore options for enhancing transformer security. The office, through two national laboratories, is funding the development of software models to assist electric utilities in modeling catastrophic outages, identifying critical network assets, and performing vulnerability assessments of those assets.[19] It is not clear how or when the OEA will transfer these modeling capabilities to industry for practical application.

State Utility Commissions. State utility officials have begun to generally address critical electric power infrastructure. In addition to cost recovery activities by the National Association of Regulatory Utility Commissioners (NARUC) critical infrastructure protection committee, a few states, such as New York, have established dedicated offices within utility commissions to address utility security issues. Several states have developed lists of critical infrastructure to share with state and federal law enforcement and security agencies.[20]

[18] Department of Defense. Naval Surface Warfare Center - Dahlgren Division. Joint Warfare Applications Department. Innovative Systems and Mission Assurance Division. Infrastructure and Interdependency Solutions Branch. Personal communication. March 5, 2004.

[19] Office of Energy Assurance, Department of Energy. "National Lab/Industry Partnership to Demonstrate Technologies for Energy Assurance." Press release. Washington, DC. October 23, 2003.

[20] National Association of Regulatory Utility Commissioners. Critical Infrastructure Committee. Cost Recovery Workshop. Meeting notes. Washington, DC. October 23. 2003.