Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism

Amy Abel
Section Research Manager

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

Dana A. Shea
Specialist in Science and Technology Policy

April 9, 2004

Congressional Research Service
7-5700
www.crs.gov
R42795

Summary

The U.S. electric power system has historically operated at such a high level of reliability that any major outage, either caused by 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 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, the 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. While occasionally causing blackouts, outages resulting from these attacks generally have not been widespread or long-lasting.

Several options exist to mitigate vulnerabilities. Several groups have long proposed the stockpiling equipment as emergency replacements for critical units that do not currently have secure spares. However, some argue that a stockpile would be costly. Another option is to standardize the designs of permanent HV transformers to facilitate emergency recovery. Some have proposed revitalizing domestic manufacturing of HV transformers arguing that a reliance on foreign manufacturers would increase recovery time due to shipping time. However, others argue that the additional shipping time is not significant compared to overall manufacturing time.

Threats against control systems may come from several different directions, such as state-sponsored attack, terrorist group attack, computer hacking, and worm or viral infection. However, the risk posed to industrial control systems from Internet-based attack is difficult to assess. Supervisory control and data acquisition (SCADA) system vulnerability reduction may be achieved through several routes, including an increase in corporate and overall cyber-security, implementation of best-practices to bolster existing security functions in control system networks, stronger oversight and enforcement of security guidelines, and new technologies for secure control systems.

Issues facing Congress include: What should be done to address vulnerabilities in the electric system? Who should be responsible for implementing appropriate actions? Who should pay? Should reliability guidelines or standards be implemented by the federal government or industry groups? And, who should be responsible for carrying out research and development to reduce vulnerabilities?

Contents

Figures

Tables

Appendixes

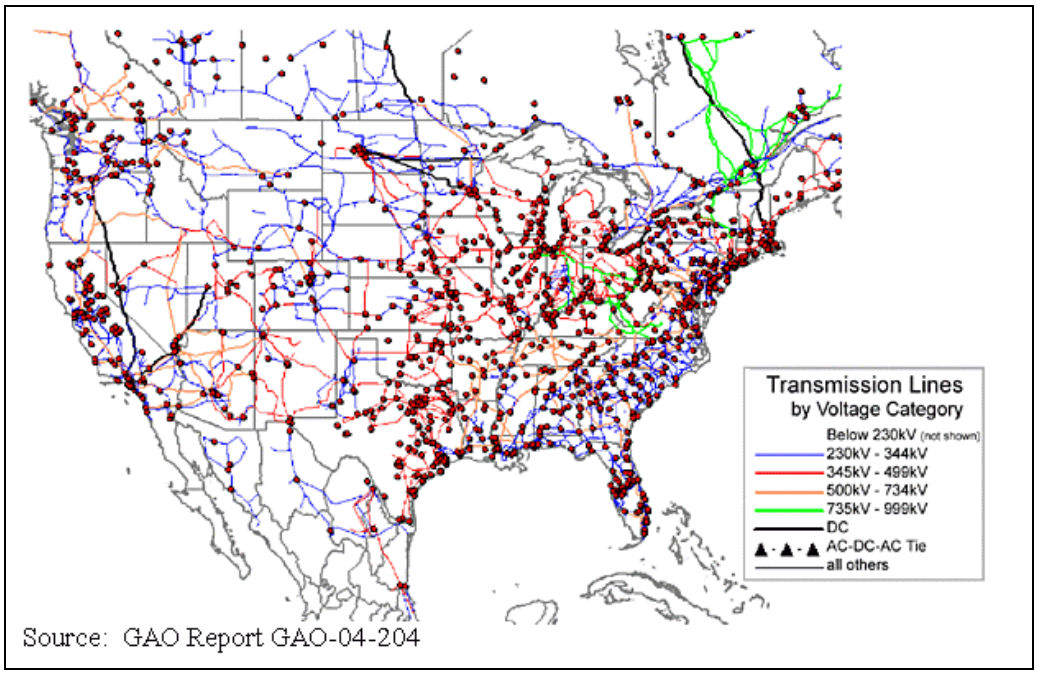
Contacts

Introduction and Overview

The U.S. electric power system has historically operated at such a high level of reliability that any major outage, either caused by sabotage, weather, or operational errors, makes news headlines. As the August 14, 2003 blackout demonstrated, a loss of electric power is very expensive and can entail considerable disruption to business, travel, government services, and daily life.

The electric utility industry operates as an integrated system of generation, transmission, and distribution facilities to deliver power to consumers. The electric power system in the United States consists of over 9,200 electric generating units with more than 950,000 megawatts of generating capacity connected to more than 300,000 miles of transmission lines; more than 247,000 miles of the transmission lines are rated at 230 kilovolts (kV) or higher (**Figure 1**).[1] In addition, approximately 150 control centers manage the flow of electricity through the system under normal operating conditions.

Figure 1. Electric Transmission Network



Most electricity in the United States is generated at power plants that use fossil fuels (oil, gas, coal), nuclear fission, or renewable energy (solar, wind, biomass). At the power plant, energy is converted into a set of three alternating electric currents, called three-phase power.[2] After power is generated, the first step in delivering electricity to the consumer is to transform the power from

[1] North American Reliability Council. Data available at: ftp://ftp.nerc.com/pub/sys/all_updl/docs/regional/MilesByVoltage.doc. Website last viewed by CRS on March 22, 2004.

[2] The three currents are sinusoidal functions of time but with the same frequency (60 Hertz). In a three phase system, the phases are spaced equally, offset 120 degrees from each other. With three-phase power, one of the three phases is always nearing a peak.

medium voltage (15-50 kV) to high voltage (138-765 kV) alternating current (**Figure 2**).[3] This initial step-up of voltage occurs in a transformer located at transmission substations at the generating facilities. High voltages allow power to be moved long distances with the greatest efficiency, i.e. transmission line losses are minimized.[4] The three phases of power are carried over three wires that are connected to large transmission towers.[5] Close to the ultimate consumer, the power is stepped-down at another substation to lower voltages, typically less than 10,000 volts. At this point, the power is considered to have left the transmission system and entered the distribution system.

Terrorist threats include physical attacks, as well as attacks on computer systems, or cyber attacks. Physical attacks could target transformers, transmission towers, substations, control centers, power plants (including nuclear reactors or dams), or fuel delivery systems. Cyber attacks could include attempts to interrupt power plant and transmission system operations, including interrupting normal water flow at hydroelectric facilities. Each of these components has vulnerabilities to a spectrum of threats ranging from weather-related incidents and vandalism to more infrequent, but potentially more devastating, acts of terrorism. Between 1987 and 1996 there were reportedly more than 20,000 recorded physical attacks on electric power targets, including power lines, substations, transformers, and central power stations, many resulting in service disruptions.[6] Most commonly, electric outages are caused by use of a weapon to shoot out transformers or use of simple tools to take down transmission towers, sometimes with the intention of causing outages but usually as a result of mischief. In contrast, no publicly reported intentional attacks on the cyber control systems have resulted in outages.

Some of these incidents are not preventable, and most utilities and regional transmission organizations have recovery plans to minimize the effect of an outage. As damaging as recent outages such as the August 2003 blackout and Hurricane Hugo have been, a planned terrorist attack could damage the electric power system well beyond the level of normal design criteria for maintaining reliability and recovery. As part of regular operating procedure, utilities make contingency plans for outages of one or two large components on their system. However, few systems make contingency plans for outages on as many as seven critical components. Under extreme scenarios, large portions the United States could be without power for several months.[7]

The potential for terrorist attack has pushed the topic of reliability into the federal policy arena from its traditional venue of being an industry responsibility, subject to state regulatory authority. Beginning in the 1990s, federal policies began emerging to ensure the protection of the nation's infrastructure, including the electric system, from terrorist activities. This report identifies physical and cyber vulnerabilities in the electric transmission and distribution system. The role of government and industry in protecting infrastructure as well as in the restoration of damaged systems is analyzed and policy implications are discussed.

[3] kV=1000 volts

[4] The loss of power on the transmission system is proportional to the square of the current (flow of electricity) while the current is inversely proportional to the voltage.

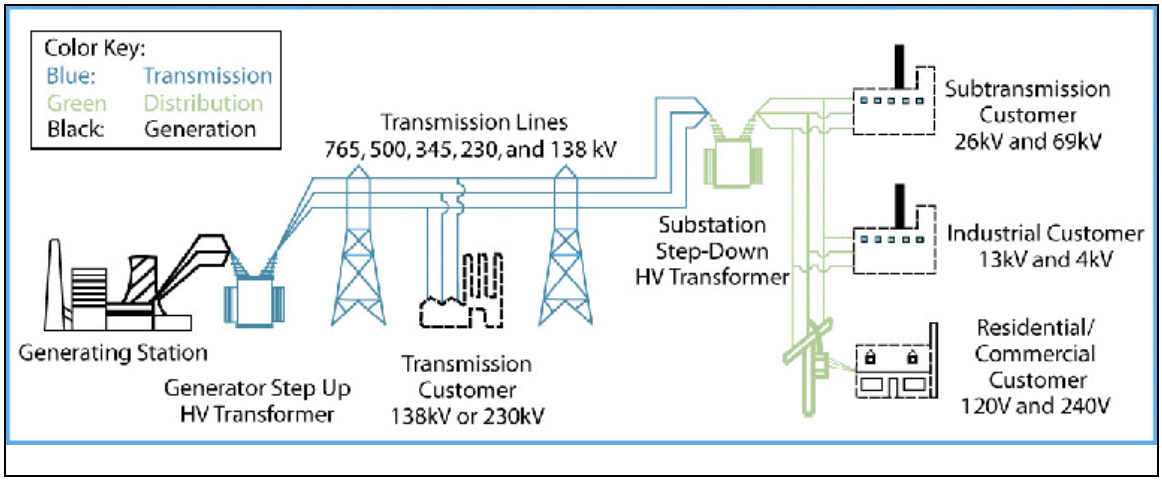
[5] Transmission towers also support a fourth wire running above the other three lines. This line is intended to attract lighting, so that the flow of electricity is not disturbed.

[6] Platts Energy Business and Technology, Vol. 5, No. 1, January/February 2000, pg. 14.

[7] Personal communication with industry official, September 18, 2003.

Regulatory Overlay

Figure 2. The Electric Power System



Source: CRS

The Federal Power Act (FPA) of 1935 established a system with the federal government regulating interstate wholesale electric transactions and state regulatory bodies having responsibility for intrastate retail transactions.[8] Under FPA, FERC oversees the rates, terms and conditions of sales of electricity for resale (wholesale transactions) and transmission service in interstate commerce.[9] However, as shown in Figures 3 and 4, FERC regulates primarily investor-owned utilities and does not have jurisdiction over federal entities, such as the Bonneville Power Administration and the Tennessee Valley Authority, cooperatives, municipalities, and the Electric Reliability Council of Texas (ERCOT).[10] States are responsible for regulating intrastate retail transactions, including the distribution of electricity. Most state regulatory commissions have major responsibility to assure that retail electric consumers have adequate and reliable electric service.[11]

Federal Initiatives

The electric utility industry is evolving to become more competitive at both the wholesale and retail level. The Energy Policy Act of 1992 (EPACT) introduced wholesale competition in the electric power industry, and subsequent FERC orders have encouraged the formation of regional

[8] U.S.C. 791a et seq.

[9] U.S.C. 824(b)(1). Under FERC Order 888, FERC asserts jurisdiction over transmission used for wholesale transactions as well as over transmission in states where the transmission services and electricity are sold separately at retail, so called "unbundled" retail sales. In New York et al. v. Federal Energy Regulatory Commission, 535 U.S. 1 (2002), the U.S. Supreme Court held that FERC has jurisdiction over transmission including unbundled retail transactions.

[10] Nebraska electric power is supplied by public power entities that are not subject to FERC jurisdiction. For a discussion of public power, see CRS report RL31477, *Public Power and Electric Utility Restructuring*.

[11] For a discussion on a utility's legal responsibilities to provide reliable and adequate service, See, *Electricity: A New Regulatory Order?* A Report prepared by the Congressional Research Service for the use of the Committee On Energy and Commerce, U.S. House of Representatives. Committee Print 102-F. June, 1991. Pgs. 223-233.

transmission organizations to facilitate access to the transmission system.[12] In addition, many states have moved to allow competition on the retail level.[13] Reliability and infrastructure protection were not addressed in federal and state restructuring legislation, and there is currently no federal regulation of electric network security. Until recently, impacts of competition on physical and cyber-security of the electric power industry were not part of the congressional debate.[14]

The potential for terrorist attacks on the electric system has pushed reliability 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 President's Commission on Critical Infrastructure Protection issued a report in October 1997 that described electric power vulnerabilities. The Commission report stated that:

> 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...[15]

In response to the Commission's report, President Clinton signed Presidential Decision Directive 63 (PDD-63) that outlines a series of actions designed to defend critical infrastructures from various threats.[16,17] 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) has assumed coordination responsibilities for the private electric utility sector. NERC retains responsibility for promulgating and overseeing reliability guidelines for the electric power industry but NERC does not have enforcement authority.[18] 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.[19]

---

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

[13] Further discussion of state retail competition see, CRS Issue Brief IB10006, *Electricity: The Road Toward Restructuring*.

[14] 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.

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

[16] See, *The Clinton's Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63,* White Paper, May 22, 1998, which can be found on http://www.usdoj.gov/criminal/cybercrime/white_pr.htm. This site was last viewed by CRS on March 22, 2004.

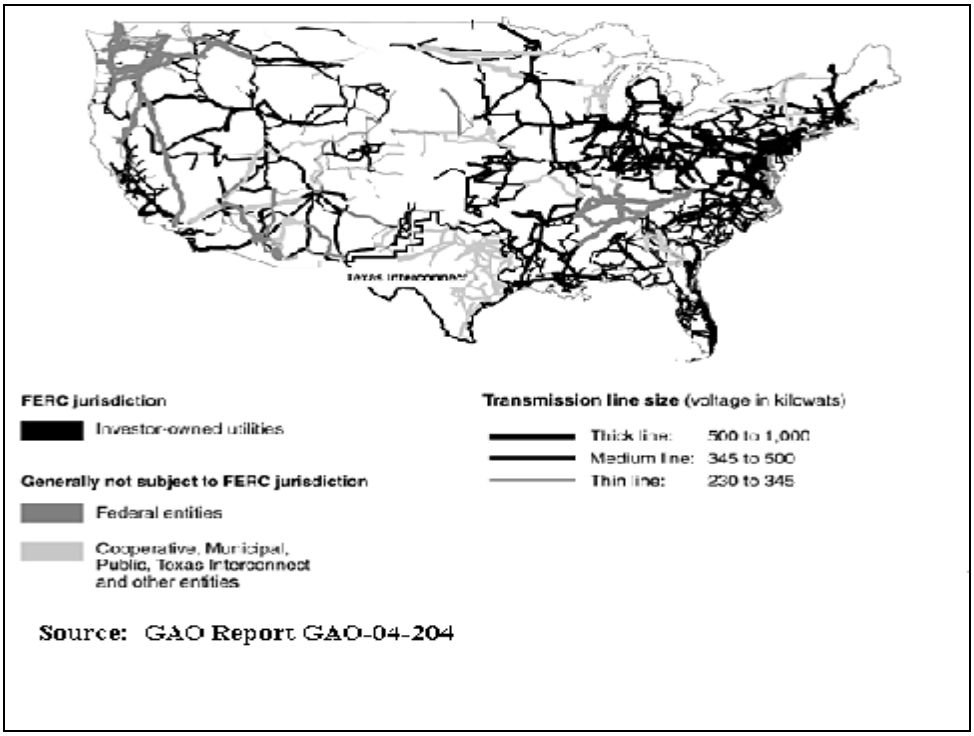
[17] For a discussion on general critical infrastructure activities, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation.*

[18] In the 108th Congress, S. 14, S. 475, S. 1754, S. 2014, S. 2095, S. 2236, the conference report on H.R. 6, H.R. 1370, and H.R. 3004 would provide for an Electric Reliability Organization to prescribe and enforce mandatory reliability standards.

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

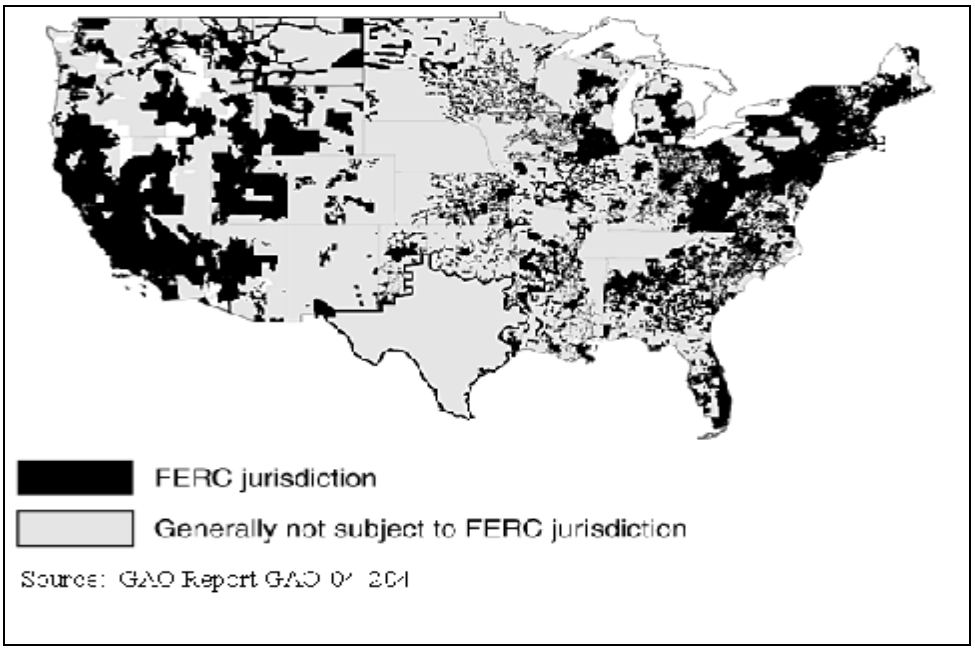
As electric utility sector coordinator, NERC functions include assessing sector vulnerabilities and developing a plan to reduce system vulnerabilities; proposing a system for identifying and averting attacks; and developing a plan to alert, contain, and deflect an attack in progress and then to reconstitute 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.[20]

Figure 3. FERC Jurisdiction of Transmission Lines



[20] See, http://www.esiac.com/

Figure 4. FERC Jurisdiction of Service Territories



Source: GAO Report

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.[21] Even though DHS and DOE have various responsibilities for infrastructure protection, they have no regulatory authority to force utilities to implement security initiatives.

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.[22] FERC's Order 630 restricts access under the Freedom of Information Act (FOIA) to certain critical energy infrastructure information (CEII) that is submitted to the Commission.[23] 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 "information that identifies the location of infrastructure." The rule also establishes

[21] 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.

[22] Another industry concern is that sharing information among utilities may raise antitrust concerns. See **Appendix B** for a legal analysis on antitrust implications of information sharing.

[23] 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.

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.[24]

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 U.S. 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, including HV transformers, 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.[25] In a speech on February 23, 2004, 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 where needed."[26]

Issues Relating to Electric Restructuring

The electric industry is shifting from an industry with guaranteed service territories and rate regulation based on costs to generate the electricity to a more competitive market.[27] As a result, several unresolved issues have emerged that relate to infrastructure security. These issues include: the availability of market information, who will pay for security investments, and the changes in use and availability of high-voltage transformers.

---

[24] CFR 388.113(c)(2).

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

[26] 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.

[27] The District of Columbia and 17 states have active restructuring plans that include retail competition. An additional 5 states have delayed retail restructuring plans.

Market Information

A competitive electric market depends on the availability of real-time information. These data inform utilities on congestion and costs of transmission and generation. Typically, the more congested a transmission corridor, the higher the price will be for electricity. A congested transmission corridor is also one that is vulnerable. Saboteurs could use publicly available market information to target vulnerable transmission corridors. Without transmission alternatives, damage to major components of a congested system would likely cause electric service disruptions.

Cost Recovery and Restructuring

Rate-regulated utilities are allowed to recover costs for investments that are both prudent and "used and useful."[28] However, in a restructured market, one issue is who will pay for security investments. States are responsible for determining how costs at retail will be allocated, and FERC's ability to encourage investment for security purposes through rate recovery is limited to investor-owned utilities involved in wholesale transactions. In a competitive wholesale electric market, utilities try to minimize costs, and in general most are not required by regulators to make investments to enhance security. On September 14, 2001, FERC notified its regulated companies that it would "approve applications proposing the recovery of prudently incurred costs necessary to further safeguard the nation's energy systems and infrastructure" in response to the terror attacks of 9/11. FERC also committed to "expedite the processing on a priority basis of any application that would specifically recover such costs from wholesale customers." Companies could propose a surcharge over existing rates or some other cost recovery method.[29] According to FERC, no transmission owners have filed formal requests for security cost recovery.[30]

Some states that allow for retail competition have imposed rate caps; in these states, cost recovery could be difficult for investments such as security enhancements. In states that have not restructured, state utility commissions determine how approved costs for investments related to infrastructure security are recovered. As reported by state utility commissions, in 2003, 25% of security related investments were driven by federal or state agency requirements and 45% were initiated by utility planning. [31] In 2003, 45% of the states received filings from utilities for recovery of security-related costs. However, state utility commissions in 83% of states do not have guidelines for determining the prudency of security investments.[32] As a result, utilities may be reluctant to invest in infrastructure security if the state has not provided clear guidance as to what investments will be considered prudent for cost-recovery purposes. To address these concerns, the National Association of Regulatory Utility Commissioners (NARUC) has established a critical infrastructure protection committee to address how regulated cost recovery can be used to encourage critical infrastructure security investments.

---

[28] *Duquesne Light Co. v. Barasch*, 488 U.S. 299, 109 S.Ct. 609 (January 11, 1989). This case makes clear that prudence is an acceptable rate methodology standard among the many available to states.

[29] Federal Energy Regulatory Commission (FERC). News release. R-01-38. Washington, DC. September 14, 2001.

[30] FERC. Personal communication. October 16, 2003.

[31] McGarvey, Joe and John D. Wilhelm. NARUC/NRRI. 2003 Survey on Critical Infrastructure Security. The National Regulatory Research Institute. October 1, 2003.

[32] *Ibid.*

Utility Industry Restructuring and High-Voltage Transformer Manufacturing

From 1950 to 1970, utility construction of large generation plants and associated transmission networks fueled a robust U.S. manufacturing market for large transformers. During this period, the United States (and Canada) accounted for approximately 40% of global demand for such units.[33] After 1970, however, utility investment in transmission infrastructure began falling off due to perceived overcapacity, public resistance to transmission siting, and greater regulatory scrutiny of capital expenditures. Beginning in the late 1980s, uncertainty about industry restructuring and the introduction of competition made grid owners even less willing to invest in new transmission.[34] This decline in U.S. transmission investment greatly reduced domestic demand for large transformers, especially high-voltage (HV) transformers. By the late 1990s, the United States and Canada accounted for only 20% of global large transformer sales.[35]

At the same time, global demand for transformers continued to grow and more foreign manufacturers entered the market. According to U.S. industry representatives, many of these foreign manufacturers benefited from dramatically lower labor costs, so they could underbid U.S. transformer makers for the remaining U.S. demand. Some of these foreign manufacturers may have been protected by import barriers which effectively closed their home markets to U.S. transformer imports.[36] While transformer tariffs today are fairly modest between the United States and key transformer trade partners, restrictive tariffs do exist in a few countries such as Brazil and Korea.[37] (**Appendix A**, **Table A-2** lists key transformer trade information for countries that have exported HV transformers to the United States.) There is no domestic manufacturing capacity in the United States for HV transformers rated 500 kV and above; Canada and Mexico have a total of four manufacturers. While the lack of domestic HV transformer manufacturers may increase delivery time, utilities have not reported difficulty in obtaining needed equipment.

Transmission System Physical Vulnerability

The main risk from a terrorist attack succeeding against the electric power industry would be a widespread power outage that lasted for an extended period of time.[38] The major components of the electric transmission system that are vulnerable to terrorist attack are transmission lines, transmission towers, transformers, and control centers. As will be discussed in this section, the most critical components of the transmission system are the HV transformers. 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.

---

[33] Newton, C., "The Future of Large Power Transformers." *Transmission & Distribution World*. September 1, 1997.

[34] See, CRS Report RL32075, *Electric Reliability: Options for Electric Transmission Infrastructure Improvements.*

[35] Newton, C., "The Future of Large Power Transformers." *Transmission & Distribution World*. September 1, 1997.

[36] White, Charles H. North American Electrical Manufacturers Association (NEMA). Remarks to the Senate Committee on Governmental Affairs, Hearings on Vulnerability of Telecommunications and Energy Resources to Terrorism. No. 101-73. Washington, DC. February 7, 1989. pgs. 65-67.

[37] U.S. Department of Commerce. International Trade Administration. Circular No. 8504.23. Summary of Tariffs and Taxes. Data on electrical transformers, static converters and inductors having a power handling capacity exceeding 100,000 kVA. October 3, 2003.

[38] Personal Communication. NERC Meeting the Security Challenge Workshop. Montreal, Québec. September 18-19, 2003.

While occasionally causing blackouts, these attacks generally have not resulted in widespread or long-lasting outages.

The industry has experienced mechanical failure of individual high-voltage transformers within a single control area resulting in blackouts lasting hours. For example, on October 23, 1997, someone with a key to a substation in San Francisco, California, illegally entered and threw 39 control switches, shutting down the substation but causing no physical damage to the transformer. 126,000 customers were without power for up to 3½ hours.[39] However, no region in the United States has experienced simultaneous failures of multiple high-voltage transformers. Experts generally agree that such a failure could cause blackouts lasting weeks and deteriorated service that could last for up to a year. The economic and social consequences of such an attack would likely be large. This section describes the critical components, their vulnerabilities, and the options available to minimize risk.

Electric Power High Voltage Transformers

High voltage transformers are a critical and vulnerable part of the nation's electric power network. High voltage (HV) units make up less than 3% of transformers in U.S. power stations, but they carry 60%-70% of the nation's electricity.[40,41] Due to the physical characteristics of HV transformers, some vulnerability will always exist, but the question is what level of security is reasonable and acceptable in the context of other infrastructure vulnerabilities. These transformers are vulnerable to terrorist attack because they are large, easily identified, and difficult to protect. Experts agree that a coordinated and simultaneous attack on multiple HV transformers could have severe implications for reliable electric service over a large geographic area, crippling its electricity network and causing widespread, extended blackouts.[42] However, such an attack would require some knowledge and sophistication on the part of potential attackers.

Restoring damaged HV transformers is difficult, since they are generally not interchangeable, they take six months or longer to build, and they must be custom ordered. Because of their enormous size and weight, transporting these units to service locations requires special rail cars or flatbed trucks. HV transformer vulnerability has been a concern for decades, but industry and federal agencies have taken only limited steps to address it.

High Voltage (HV) Transformer Characteristics

Utility transformers control the voltage of electricity so that it can be synchronized with other power supplies, transmitted long distances, and distributed to customers. Transformers range in size from small, pole-mounted units that serve a dozen homes to transmission units that serve an entire city. The larger the transformer, the higher the voltage the transformer can handle. Utility

[39] NERC maintains a database of power disturbances. The database can be found at: http://www.nerc.com/~dawg/

[40] Newton, C. September 1, 1997.

[41] Loomis, William M. Strategic Partners-Technical Systems, consulting engineer. "Super-Grid Transformer Defense: Risk of Destruction and Defense Strategies." Presentation to NERC Critical Infrastructure Working Group, Lake Buena Vista, FL. December 10-11, 2001.

[42] Personal Communication. NERC Meeting the Security Challenge Workshop. Montreal, Québec. September 18-19, 2003.

transformers, regardless of size, fundamentally consist of copper wire wrapped around a metallic "core" within an insulated protective housing covered with a 5/8 to 3/4-inch mild steel tank. They are linked to the electricity network by protruding metal and ceramic connectors called "bushings" which resemble giant spark plugs. Larger transformers generate considerable waste heat during operation, so they are cooled by a system of internally circulating oil and external radiators, analogous to the cooling system in a car engine. Transmission transformers are located in network substations along with transmission lines, associated electric equipment, and system controls. These substations may be found in remote locations or near urban centers, depending upon regional transmission needs. Many are located alongside electric generation plants, linking those plants to the transmission network.

High-voltage transformers (units between 345 kV and 750 kV capacity) are physically large and extraordinarily heavy. **Figure 5**, for example, shows a new 345 kV transformer many times larger than the vehicle nearby. This unit weighs 435 tons, including 29,000 gallons of cooling oil.[43] (Note that the vertical bushings are not yet connected to transmission lines because the unit is being moved.) Generally, the higher the transformer's voltage, the larger the transformer. For example, American Electric Power (AEP) has a 750 kV transformer bank that is several stories tall and covers an area of 60 by 90 feet.[44]

Figure 5. 345 kV Transformer Installation

Source: Pauwels Canada.

Manufacture

Most HV transformers are designed and manufactured to custom specifications for a specific network application. This manufacturing process takes a minimum of six to twelve months, including three to four months for the engineering design.[45] Since manufacturing generally occurs

[43] Pauwels Canada, Inc. Personal communication. October 20, 2003.

[44] American Electric Power (AEP).

[45] North American Reliability Council. Data available at: ftp://ftp.nerc.com/pub/sys/all_updl/docs/regional/MilesByVoltage.doc. Website last viewed by CRS on March 22, 2004.

on a single production line with just-in-time component supplies, advanced production scheduling is important for managing delivery.[46] Physical assembly is labor intensive, requiring manual winding of the copper wire around the transformer core and frequent engineering checks during manufacturing. Extensive testing of completed units also contributes to HV transformer manufacturing time.

The installed cost for an HV transformer depends heavily on its configuration and specific design requirements. For example, AEP spent nearly $15 million for the 750 kV substation, but most installations are smaller and therefore less costly.[47] According to one Canadian manufacturer, the average factory prices for large 345 kV and 500 kV units are in the $3-$5 million range, before transportation and installation costs.[48]

Inventory

Approximately 4,000 HV transformers operate in the United States.[49] Investor-owned utilities own most of these, although government-owned utilities such as the Bonneville Power Administration, Tennessee Valley Authority, Western Area Power Administration, and the Los Angeles Department of Water and Power own many HV transformers as well. HV substation information for specific investor-owned utilities is publicly available in annual reports filed with the Federal Energy Regulatory Commission (FERC).[50] For illustrative purposes, CRS compiled these public data, along with data obtained directly from public utilities, to identify the general locations of the largest HV transformers in the United States. **Figure 6** shows the number of 500 kV and 750 kV transformer *substations* this analysis identified (each substation may have multiple HV transformers) within the ten regional reliability councils coordinated by the North American Electric Reliability Council (NERC). While **Figure 6** shows only the highest voltage transformer substations, 345 kV and lower voltage stations are also listed in FERC filings. These lower voltage transformers could be critical depending on a region's specific network characteristics.

Criticality of HV Transformers

Because they carry so much electricity, the destruction of HV transformers can seriously reduce the transmission capacity of a regional electric power network and lead to extended blackouts. The impact of such a failure would depend on the electricity flows in that part of the network, congestion from major network bottlenecks, and the status of other key facilities such as power plants, transmission lines, and other substations. Power grid planners generally anticipate the possible loss of a single HV transformer substation and are prepared to reroute power flows as necessary to maintain regional electric service.[51] But the simultaneous loss of multiple HV

[46] The three currents are sinusoidal functions of time but with the same frequency (60 Hertz). In a three phase system, the phases are spaced equally, offset 120 degrees from each other. With three-phase power, one of the three phases is always nearing a peak.

[47] kV=1000 volts

[48] The loss of power on the transmission system is proportional to the square of the current (flow of electricity) while the current is inversely proportional to the voltage.

[49] Transmission towers also support a fourth wire running above the other three lines. This line is intended to attract lighting, so that the flow of electricity is not disturbed.

[50] Platts Energy Business and Technology, Vol. 5, No. 1, January/February 2000, pg. 14.

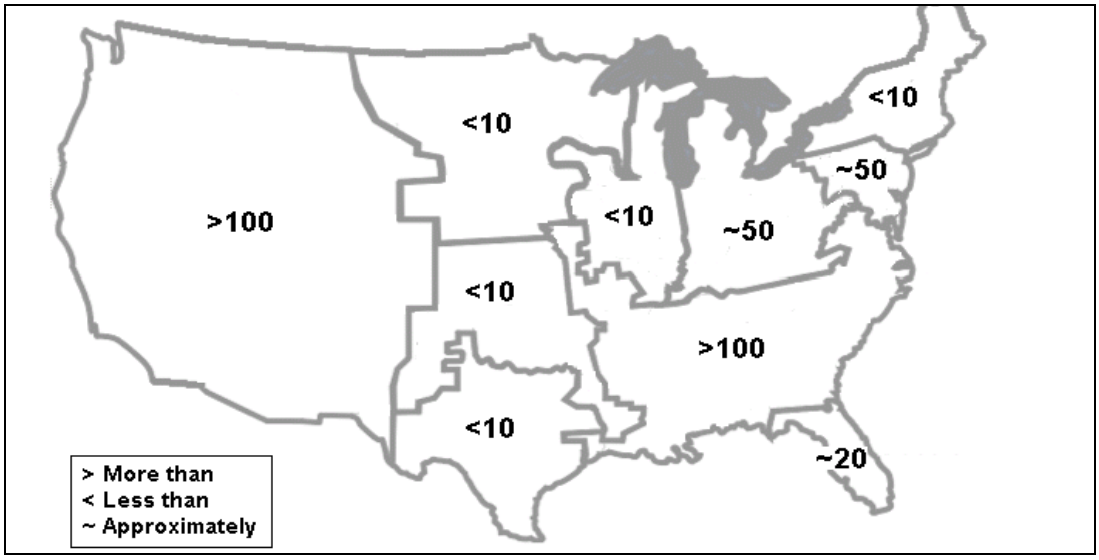
[51] Personal communication with industry official, September 18, 2003.

transformers, especially in a constrained transmission area, could exceed the capability of a regional network to reroute power through secondary lines. In 1990, the Congressional Office of Technology Assessment (OTA) completed a study on the physical vulnerability of the electric power system and found that:

> In most cases, the nearly simultaneous destruction of two or three transmission substations would cause a serious blackout of a region or utility, although of short duration where there is an approximate balance of load and supply.... The destruction of more than three transmission substations would cause long-term blackouts in many areas of the country.[52]

In such an emergency scenario, limited electric service could likely be restored in the short term by imposing "rolling" blackouts, rerouting transmission, and using portable transformers. Nonetheless, an extended loss of key HV substations would leave the regional network crippled and highly susceptible to further disturbance.[53] According to power industry experts, certain parts of the U.S. transmission network are particularly vulnerable to HV substation failure. These areas have severely constrained transmission paths relying on a small number of HV transformers in extremely critical network locations.

Figure 6. Estimated Number of 500 kV or Larger Transformer Substations by NERC Region



Sources: NERC, FERC, BPA , WAPA, TVA, NYPP.

[52] U.S.C. 791a et seq.

[53] U.S.C. 824(b)(1). Under FERC Order 888, FERC asserts jurisdiction over transmission used for wholesale transactions as well as over transmission in states where the transmission services and electricity are sold separately at retail, so called "unbundled" retail sales. In New York et al. v. Federal Energy Regulatory Commission, 535 U.S. 1 (2002), the U.S. Supreme Court held that FERC has jurisdiction over transmission including unbundled retail transactions.

Vulnerability of HV Transformers

All HV transformers are designed to withstand severe operational conditions such as lightning strikes, hurricanes, and network power fluctuations—but they are vulnerable to terrorist attacks. Despite their great size and internal complexity, HV transformers can be readily disabled or destroyed. According to one manufacturer, "if someone were to intentionally try ... it is a surprisingly simple task and there are a large number of ways to conceivably damage a transformer beyond repair."[54] Transformer experts have asserted that a bad actor with basic knowledge of transformer design could inflict irreparable damage.[55] Such attacks can cause massive electrical short circuits and oil fires that would destroy an HV transformer and damage surrounding infrastructure. A recent fire at a 345 kV transformer in Texas, for example, destroyed the transformer and burned for five hours and "caused plumes of smoke that could be seen for miles."[56] In addition to direct attacks on the transformers themselves, HV substations can be further disabled by damaging associated transmission lines or control centers that may be located on site.

Because HV transformers are so big and are connected to the largest overhead transmission towers, they are easily identified along major transmission corridors. High voltage transformers are usually housed in substations that are enclosed with a chain-link fence. Guards are not often stationed at these facilities. Consequently, HV transformers are easier to access than other critical electric facilities such as generation plants and control centers. Increasingly, utilities are using closed-circuit surveillance and other methods to detect intrusion. However, access to the substation may be by either cutting or scaling the chain-link fence. Once inside, a saboteur could cause damage by accessing the control room or physically damaging the HV transformer. Penetrating the 5/8 to 3/4 inch mild steel tank with any device could short-circuit the windings and irreparably destroy the transformer. Alternatively, a saboteur could attempt to open a valve and drain the insulating oil. Lighting a road flare and igniting the oil might cause the transformer to arc and eventually explode.[57]

A terror group could, without significant training, identify critical HV transformer locations and time an attack for greatest effect. This could be accomplished with basic knowledge of transmission operations and regional network characteristics drawn from publicly available sources, including electric marketing data indicating constrained areas of the network.[58] The 1990 OTA report describes such a scenario:

> (One) example is a city served by eight transmission substations spread along a 250-mile line and located in five States. A knowledgeable saboteur would be needed to identify and find the eight transmission substations. A highly organized attack would also be required.

[54] Nebraska electric power is supplied by public power entities that are not subject to FERC jurisdiction. For a discussion of public power, see CRS report RL31477, *Public Power and Electric Utility Restructuring*.

[55] For a discussion on a utility's legal responsibilities to provide reliable and adequate service, See, *Electricity: A New Regulatory Order?* A Report prepared by the Congressional Research Service for the use of the Committee On Energy and Commerce, U.S. House of Representatives. Committee Print 102-F. June, 1991. Pgs. 223-233.

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

[57] Further discussion of state retail competition see, CRS Issue Brief IB10006, *Electricity: The Road Toward Restructuring*.

[58] 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.

> However the damage would be enormous, blacking out a four-State region, with severe degradation of both reliability and economy for months.[59]

In 1997, the Irish Republican Army reportedly planned this same kind of coordinated attack against six transmission substations in the United Kingdom. Although the attack was prevented, had it been successful it could have caused serious and widespread power outages in London and the South East of England for months.[60]

It is relatively easy to learn about HV transformer vulnerabilities from engineers and operators experienced with this technology. Several transformer experts provided CRS with detailed descriptions of numerous "simple" ways terrorists could destroy HV transformers. Despite the sensitive nature of such information, many of these experts did not attempt to verify our identities or challenge our interest in this particular topic. General transformer sabotage information is also available on the Internet. One white supremacist site, for example, includes the following text in its on-line sabotage manual:

> The power generation and distribution systems of most major Western cities are surprisingly vulnerable.... Attacking during peak consumption times (Winter in cold climates and Summer in hot climates) will make power diversion impossible.... Arson, explosives or long-range rifle fire can be used to disable substations, transformers and suspension pylons. A simultaneous attack against a number of these targets can shut down power ... with the advantage that service cannot be quickly restored by diverting power from another source. Each broken link in the power grid must be repaired in order to fully restore service. An individual, equipped with a silenced rifle or pistol, could easily destroy dozens of power transformers in a very short period of time.

The site also includes photographs of a large transformer substation, a small distribution transformer, and other electric power infrastructure.[61]

It is very difficult to restore service from a damaged HV transformer substation. As noted above, transmission experts assert that most HV transformers currently in service are custom designed and, therefore, cannot be generally interchanged. Furthermore, at $3-5 million per unit or more, most utilities find it too costly to maintain large inventories of spare HV transformers solely as emergency replacements, so few extras are on hand. One regional transmission control area, for example, maintains 11 spares for 135 HV transformers on its system—a typical ratio.[62] The Tennessee Valley Authority's inventory of 500 kV transformers includes one spare for every three units in service. This high number of spares is not typical among HV transformer owners. Furthermore, TVA has standardized its transformer specifications more than most utilities.[63] Most

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

[60] See, *The Clinton's Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63,* White Paper, May 22, 1998, which can be found on http://www.usdoj.gov/criminal/cybercrime/white_pr.htm. This site was last viewed by CRS on March 22, 2004.

[61] For a discussion on general critical infrastructure activities, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation.*

[62] In the 108th Congress, S. 14, S. 475, S. 1754, S. 2014, S. 2095, S. 2236, the conference report on H.R. 6, H.R. 1370, and H.R. 3004 would provide for an Electric Reliability Organization to prescribe and enforce mandatory reliability standards.

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

HV transformer spares are located directly alongside operating units because the spares were originally intended for replacements due to mechanical failure, not terrorist attack. As a result, the spares themselves are also vulnerable to terrorist attack.

The United States currently has no manufacturers of 500 kV or 750 kV transformers, and only two manufacturers of 345 kV units. At least one U.S. manufacturer of lower voltage transformers contends it could start an HV transformer production line within a year, but it would need substantial startup capital and a sufficient flow of orders to do so.[64] (**Appendix A**, **Table A-1** lists global HV transformer manufacturers.)

Within the United States, transportation of these transformers is difficult. Due to their size and weight, most HV transformers are transported over land on special railcars which have up to 36 axles to distribute the load. There are only 15 of these railcars in the Unites States, which can present a logistical problem if they are needed in a transformer emergency.[65] Some specialized flatbed trucks can also carry heavy transformer loads over public roadways, but the few such trucks that exist have less carrying capacity and greater route restrictions than the specialized railcars do. Many of the route restrictions appear to exist because HV transformers exceed highway weight limits.

HV Transformer Vulnerability In Perspective

There is widespread agreement among government, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack could have catastrophic consequences. But there is also widespread acknowledgment that the most serious, multi-transformer attacks would require acquiring operational information and a certain level of sophistication on the part of potential attackers. The nation's HV transformers have been vulnerable for decades and have not been attacked in the coordinated way described in this report. Vandals, labor protesters, and environmental groups in the United States have deliberately damaged transformers on a number of occasions resulting in some hours-long disruptions, yet these incidents have not caused months-long regional blackouts that are of concern with a simultaneous attack of several transformers.[66] Utilities have also responded to numerous failures of individual HV substations from conventional operational causes without extensive negative effects on the overall electric power network. Consequently, despite the technical arguments in this report, some analysts question whether U.S. HV transformer security concerns may be overstated. Without more specific information about potential targets and attacker capabilities, this remains an open question. As policy makers seek to establish the best policies to address HV transformer vulnerability relative to other infrastructure security priorities, understanding this vulnerability in the context of specific demonstrable threats may become increasingly important.

[64] See, http://www.esiac.com/

[65] 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.

[66] Another industry concern is that sharing information among utilities may raise antitrust concerns. See **Appendix B** for a legal analysis on antitrust implications of information sharing.

Control Center Characteristics and Physical Vulnerabilities

The flow of electric power in the United States is managed by nearly 150 control centers. (Red dots in **Figure 1** illustrate the locations of control centers in North America.) Control centers are operated by either a single utility or for multi-utility systems such as the PJM Interconnection. A control center monitors generating plants, the transmission and distribution system, and customer demand within a control area. People monitor and operate a highly automated computer system designed to remotely control field equipment such as generators and switches. Communications between a control center and field equipment generally occur over utility-owned communications networks consisting mostly of analog and digital microwave technology and fiber optic lines.[67] Most control rooms contain a large map board to visually display which circuits are closed or open, and the status of key power plants and substations.

Few utilities maintain back-up control centers for use if the primary control center is destroyed or disabled. When they do exist, these back-ups are generally located a few miles from the primary control center to facilitate the movement of trained personnel. CRS is not aware of any utility that operates a manned back-up control center.[68]

Restructuring in the electric utility industry has resulted in changes in transmission system control. Some areas of the country have consolidated the control function to a single control center. For example, the California Independent System Operator (CAISO) began operation in 1998 and controls the flow of electricity for 75% of the state although the ownership of the transmission lines is retained by the utilities. Prior to 1998, the three major utilities owned and separately operated segments of the transmission system. According to the CAISO, there are 15 operators on shift around-the-clock, eleven of whom are located in the Folsom Control Center and four in an additional control center in Southern California. The CAISO maintains a satellite backup control room for use in emergencies in Alhambra, approximately 400 miles from Folsom. The CAISO also maintains four redundant computer systems.[69] As a comparison, the Midwest ISO, which began operation as a Regional Transmission Organization (RTO) in 2001, provides reliability coordination for 37 control areas in 15 states, each operating separate control centers. The Midwest ISO has not announced plans to consolidate the control operations.[70]

Centralized control operations and multiple control centers within a region present different security concerns. During normal operations and during emergencies when generation and transmission assets become unavailable to the system, some transmission operators argue that a regional centralized control center can most efficiently operate the system.[71] With multiple control centers, communication between control areas is more difficult.

Rather than relying on computers to manage the regional system, the Midwest ISO relies on telephone communication between control areas. This was problematic during the hours before

---

[67] 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.

[68] CFR 388.113(c)(2).

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

[70] 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.

[71] The District of Columbia and 17 states have active restructuring plans that include retail competition. An additional 5 states have delayed retail restructuring plans.

the August 2003 blackout. The U.S.-Canada Power System Outage Task Force found that First Energy violated five NERC reliability standards. One violation was that First Energy did not notify other control centers of an impending system emergency.[72] However, there are operational advantages to multiple control centers within a region. If an individual control center in an area such as the Midwest ISO goes out of service for some reason, and the control area is isolated from neighboring operations, degradation of service would be limited to those customers served by the control area. As a contrast, customers in an entire region dependent on a centralized control center could experience service degradation or blackouts if their control center were unable to operate.

Control centers are located in structures that in most cases have enhanced security compared to most office buildings but may be co-located with other utility offices and operations. Typically, control rooms limit access to cleared employees and doors are secured with carded entry. The main physical security concern is that an intruder will gain access to the control center, and either take over the system controls or force utility personnel to operate the system in a manner that causes significant damage to utility infrastructure and causes long-term blackouts. If a control center is physically damaged or destroyed either from natural causes (earthquakes, storms) or intentional attack, most control operations could be handled manually at the power plant or from other locations. However, manual operation is at best less efficient than computer controlled-operations and at worse could result in degradation of service. CRS was told by several utility personnel that one concern is that control center operators with experience operating the control system manually are nearing retirement. Most newer control center employees have never operated the system without the benefit of computers.[73]

Transmission Tower Characteristics and Vulnerabilities

Large steel structures called transmission towers support high-voltage transmission lines. Transmission towers and lines are inherently vulnerable to physical damage. They are not well protected and are easily seen from the air and ground. However, system disturbances that could result from multiple damaged transmission towers are significantly less than what could occur with multiple HV transformer failures or control center failures.

Ice storms, hurricanes, and other natural disasters frequently cause lines and towers to fall or be damaged. In addition, malicious damage (e.g., shooting insulators) and sabotage are reoccurring problems for transmission owners and operators. In October 2003, a saboteur removed support bolts at the base of twenty high-power transmission towers in the Pacific Northwest. The suspect surrendered to police on November 2, 2003, and later admitted to the crime; he was sentenced to 27 months in prison and ordered to pay $37,000 in restitution. At his sentencing, the saboteur said he was trying to point out the power system's vulnerability.[74]

Reinforcing transmission towers has not been a priority for the industry, since most towers are not considered critical infrastructure. Unlike HV transformers, there are several domestic manufacturers of tubular steel transmission towers. They are transportable in sections and do not

[72] *Duquesne Light Co. v. Barasch*, 488 U.S. 299, 109 S.Ct. 609 (January 11, 1989). This case makes clear that prudence is an acceptable rate methodology standard among the many available to states.

[73] Federal Energy Regulatory Commission (FERC). News release. R-01-38. Washington, DC. September 14, 2001.

[74] FERC. Personal communication. October 16, 2003.

require specially designed vehicles for transportation. Most utilities maintain some spares. However, according to one utility expert, utilities do not maintain spares of large (300-400 foot) towers, and these can take between several weeks and 6 months to replace. This is of particular concern at large river crossings.[75] Several towers in an area could be damaged without power disruption or with minimal power outages. Breakers, switches, and jumpers connect and disconnect portions of the system to minimize power disruptions. Alternate lines can provide a backup path for the delivery of power while structures are down and restoration is underway.[76] However, in areas of severe transmission congestion, alternative paths for power flow may not exist. A strategic attack on several towers in these areas might cause significant deterioration of service and blackouts.

Industry Security Initiatives—Physical Infrastructure

NERC has developed voluntary guidelines for electric network security which include general recommendations for the protection of critical facilities such as HV transformer substations. These recommendations address fencing, locks, personnel identification, alarms, surveillance equipment, vehicle barriers, projectile barriers, lighting, signage, and security awareness training.[77] Utilities have begun implementing these types of measures throughout their networks, particularly around their most critical assets such as HV transformer substations.[78] NERC also maintains a national database of spare transformers, is creating protocols for equipment sharing, and is developing recovery strategies for terrorist attacks on transformers and other critical assets.[79] However, NERC has no authority to enforce any security guidelines.

The Electric Power Research Institute (EPRI), an industry-funded energy research consortium, is also addressing HV transformer vulnerabilities. In cooperation with NERC, EPRI has been developing conceptual designs for "recovery transformers" which would enable rapid temporary replacement of damaged HV transformers. Recovery transformers could operate at multiple voltage ratings and be sized to allow for transport by rail, truck, or cargo plane from strategic U.S. storage locations.[80] EPRI is also developing new vulnerability assessment procedures that "identify and rank critical simultaneous multi-station contingencies, which might be expected from a coordinated terrorist attack."[81]

Some regional transmission control centers are now routinely performing contingency analysis on the regional networks they manage to better prepare for possible terrorist attacks. The PJM Interconnection, for example, models on both a day-ahead and real-time basis the potential loss of several critical nodes simultaneously in the PJM network. PJM's contingency analysis ranks the

[75] McGarvey, Joe and John D. Wilhelm. NARUC/NRRI. 2003 Survey on Critical Infrastructure Security. The National Regulatory Research Institute. October 1, 2003.

[76] *Ibid*.

[77] Newton, C., "The Future of Large Power Transformers." *Transmission & Distribution World*. September 1, 1997.

[78] See, CRS Report RL32075, *Electric Reliability: Options for Electric Transmission Infrastructure Improvements.*

[79] Newton, C., "The Future of Large Power Transformers." *Transmission & Distribution World*. September 1, 1997.

[80] White, Charles H. North American Electrical Manufacturers Association (NEMA). Remarks to the Senate Committee on Governmental Affairs, Hearings on Vulnerability of Telecommunications and Energy Resources to Terrorism. No. 101-73. Washington, DC. February 7, 1989. pgs. 65-67.

[81] U.S. Department of Commerce. International Trade Administration. Circular No. 8504.23. Summary of Tariffs and Taxes. Data on electrical transformers, static converters and inductors having a power handling capacity exceeding 100,000 kVA. October 3, 2003.

most critical network assets (power plants, substations, transmission lines, etc.) on any given day and identifies operational changes to reduce the network's dependence on those assets should they be unexpectedly disabled. PJM believes this analysis reduces the overall vulnerability of the transmission network to terrorist attacks and would assist in restoration efforts if an attack takes place.[82] Not all transmission operators have this level of contingency modeling in place, however, and there is no government or industry requirement for it.

Government Security Initiatives—Physical Infrastructure

Department of Homeland Security

The Department of Homeland Security (DHS) has been addressing HV transformer security within its Protective Security Division (PSD) but currently is not addressing transmission towers or control center security. The 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."[83] The program is initially focused on HV transformers, although it will include other types of electrical equipment in the future. As part of this spares program, PSD is building upon EPRI's transformer activities to develop a "containerized" HV recovery transformer which could fit in a conventional International Standards Organization (ISO) 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.[84] 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.[85] PSD expects designs for the containerized transformers to be completed in 2004.

According to PSD, in 2004 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 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.[86] DHS is also developing grid monitoring capability. DHS did not respond to repeated attempts by CRS to obtain information on the status of this program.

[82] Personal Communication. NERC Meeting the Security Challenge Workshop. Montreal, Québec. September 18-19, 2003.

[83] NERC maintains a database of power disturbances. The database can be found at: http://www.nerc.com/~dawg/

[84] Newton, C. September 1, 1997.

[85] Loomis, William M. Strategic Partners-Technical Systems, consulting engineer. "Super-Grid Transformer Defense: Risk of Destruction and Defense Strategies." Presentation to NERC Critical Infrastructure Working Group, Lake Buena Vista, FL. December 10-11, 2001.

[86] Personal Communication. NERC Meeting the Security Challenge Workshop. Montreal, Québec. September 18-19, 2003.

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 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.[87]

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 HSPD-7. The OEA has expressed concern about HV transformer vulnerability and general 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.[88] It is not clear how or when the OEA will transfer these modeling capabilities to industry for practical application. The OEA has not taken any other formal actions specifically related to HV transformers.

State Utility Commissions

State utility officials have begun to generally address critical electric power infrastructure. In addition to cost recovery activities by NARUC's 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.[89]

Cyber Systems in the Electric Utility Industry

The potential of cyber-threats causing damage to electric utilities has garnered increasing attention over the past several years. Since electric utilities, along with other "brand name" companies, are high profile targets for hackers and cyber-vandals, the cyber-security of these companies is an area of concern. If cyber-attacks or intrusions can cause failure of electric service, or cause an extended electric outage, rectifying systemic weaknesses may be a national priority. Sources have indicated that the rate and number of cyber-attacks on electric utilities are currently high and continue to increase. Whether these cyber-attacks are malicious or merely general scanning activities, their high volume concerns some cyber-security experts.

[87] Pauwels Canada, Inc. Personal communication. October 20, 2003.

[88] American Electric Power (AEP).

[89] North American Reliability Council. Data available at: ftp://ftp.nerc.com/pub/sys/all_updl/docs/regional/MilesByVoltage.doc. Website last viewed by CRS on March 22, 2004.

In addition to common business concerns related to cyber-security, such as data security and electronic theft, electric utilities have potential cyber-vulnerabilities of greater concern to the general populace. Because of the greater degree of automation and computer control in electric utilities, the ability of an electric utility to provide and maintain electric service could be compromised by cyber-attacks that target industrial control systems or through a cyber-attack that significantly degrades the ability of these computerized systems to process commands and signals. As a result, some experts believe that, in addition to protection of corporate systems from cyber-attack, the vulnerabilities present in control system architecture must be directly addressed. In 1997, the President's Commission on Critical Infrastructure Protection report stated,

> From the cyber perspective, SCADA [supervisory control and data acquisition] systems offer some of the most attractive targets to disgruntled insiders and saboteurs intent on triggering a catastrophic event. With the exponential growth of information system networks that interconnect the business, administrative, and operational systems, significant disruption would result if an intruder were able to access a SCADA system and modify the data used for operational decisions, or modify programs that control critical industry equipment or the data reported to control centers.[90]

Electric Utility Cyber Characteristics and Vulnerabilities

Electric utilities, like other businesses, have increased their cyber-security in response to known threats and vulnerabilities. Some have hired security officers in charge of physical and/or cyber-security issues. As in most industrial sectors, the rate of intrusions by hackers or other persons into the corporate computer systems is undisclosed, as there is no mandatory reporting requirement for such intrusions. However, some incidents have been publicized, either by industry members or through the general press, which have documented cases of cyber-intrusion into electric utilities. These incidents have included hacking into corporate systems of CAISO,[91] infecting utility-owned nuclear power plant systems,[92] and infecting electric management systems themselves.[93] Cyber-vulnerability continues to exist to some degree within the electric utilities.

SCADA systems are often used for remote monitoring over a large geographic area and transmitting commands to remote assets. In the electric sector, these systems must operate with very short response times and provide information to generate feedback from operators or other computer systems. Some SCADA systems use publicly owned networks to transfer information or use wireless transmission to actuate remote equipment. Some SCADA systems use plain text, rather than encrypted, messaging as their transmission mode, generally because of time constraints related to decoding and encoding encrypted messages. In addition, older switches are unable to handle encryption. Some electric utility control system components are relatively slow and marginal—extra computation, such as encryption/decryption, would degrade their performance as a control system component. Often, control systems distributed over large

[90] The three currents are sinusoidal functions of time but with the same frequency (60 Hertz). In a three phase system, the phases are spaced equally, offset 120 degrees from each other. With three-phase power, one of the three phases is always nearing a peak.

[91] kV=1000 volts

[92] The loss of power on the transmission system is proportional to the square of the current (flow of electricity) while the current is inversely proportional to the voltage.

[93] Transmission towers also support a fourth wire running above the other three lines. This line is intended to attract lighting, so that the flow of electricity is not disturbed.

geographic distances contain built-in modems for remote troubleshooting. Improperly configured modems, with weak security, could be points of entry directly into a control system network.[94]

The networking of industrial control systems on a greater scale has led to increased synergy and efficiency, and real time information from these systems is increasingly important for marketing purposes. Originally, control systems and corporate networks were separate. However, as electric utility industry restructuring has evolved, real-time information flow is needed between the control systems and corporate offices for marketing purposes. Consequently, some control system computers are becoming linked to corporate computer systems, potentially making them vulnerable to cyber-attack through the Internet. Some of these linkages are well-understood and well-protected, but others may have been initially established for maintenance or other purposes but not subsequently removed, or intentionally established without the knowledge of security officials (usually non-work related connections such as internet games), and may be points of cyber-security vulnerability for the control system network.

It is clear from the available literature that electric utility corporate computers, as well as the corporate computer systems of other utilities, are increasingly under cyber-attack. An important distinction should be drawn between penetration of the corporate network and penetration of the control system network. Gaining access to the corporate computer network, while potentially compromising valuable information, does not necessarily equate to gaining access to the control system network and compromising the systems controlling sections of the electric power grid.

While there are financial ramifications present in the increased vulnerability of corporate networks, it is considered unlikely that an attack solely targeting corporate systems would result in any degradation of electric grid operation.[95] Because the degree of integration between control system networks and corporate networks is difficult to judge from the available literature, it is unclear what the likelihood is that a given intruder could transfer from the corporate networks to the control system network. While there are documented examples of penetration of corporate networks, there are few examples of penetration of control system computers from the Internet. Most cases where there has been successful penetration of the control system computers have involved insider access to these systems. In contrast, the Department of Energy and the Department of Defense have performed vulnerability assessments, through "red team" exercises,[96] for some individual stakeholders in critical infrastructure industries.[97] General reports have indicated that many of these "red team" exercises have resulted in successful compromise of some systems.

Threat to Cyber Systems

The threats posed by adversarial forces against control systems has not been generally reported in unclassified literature. However, it is generally known that threats against control systems could

[94] Platts Energy Business and Technology, Vol. 5, No. 1, January/February 2000, pg. 14.

[95] Personal communication with industry official, September 18, 2003.

[96] U.S.C. 791a et seq.

[97] U.S.C. 824(b)(1). Under FERC Order 888, FERC asserts jurisdiction over transmission used for wholesale transactions as well as over transmission in states where the transmission services and electricity are sold separately at retail, so called "unbundled" retail sales. In New York et al. v. Federal Energy Regulatory Commission, 535 U.S. 1 (2002), the U.S. Supreme Court held that FERC has jurisdiction over transmission including unbundled retail transactions.

come from several different directions, such as state-sponsored attack, terrorist group attack, hacking, and worm or viral infection.

Some experts believe that nation-states have sponsored groups within their countries, or enlisted parts of their armed forces infrastructure, to develop the capability to perform cyber-attacks. China, Russia, and North Korea, among others, have been identified as countries that have developed or are developing capabilities in cyber-warfare.[98] Indicators of the possibility that terrorist organizations are attempting to develop such a capability include the discovery of a training facility in Afghanistan, reportedly linked to al Qaeda, and the increased activities of hackers sympathetic to terrorist causes.[99]

The degree to which these countries and organizations are prepared to launch an attack that would compromise critical infrastructure has not been reported in the public literature. The Federal Bureau of Investigation (FBI) has testified that, "The FBI assesses the cyber-threat to the U.S. to be rapidly expanding, as the number of actors with the ability to utilize computers for illegal, harmful, and possibly devastating purposes is on the rise."[100] Following the August 2003 electric blackout, the Federal Bureau of Investigation testified that, "The FBI has received no specific, credible threats to electronic power grids in the United States in the recent past ...."[101] While targeted cyber-attacks on electric utility control systems remain a possibility, published reports of their occurrence have not appeared in the open literature.

Cyber Vulnerability Reduction

The risks posed to industrial control systems from Internet-based attack is difficult to assess. Consequently, many focus on reducing the vulnerabilities that are known, with the hope of reducing the associated risk. An approach taken by some companies has been to increase the quality of corporate network security systems, to block initial intrusion through the Internet.[102] Such an approach has been criticized by some as protecting only against external threats and as not addressing the actual vulnerabilities inherent in control systems themselves. Also, this approach would not protect against attacks directed at the control system network through maintenance modems or other direct access equipment.

Several approaches are used to reduce the vulnerability of control system computer networks. The concept of security by obscurity has been historically used, with highly customized, proprietary control system architectures being common. This assertion has been challenged by security analysts who contend that industrial control systems are significantly less obscure now than when proprietary systems were the norm.[103] Foreign utility companies increasingly use current off-the-

---

[98] Nebraska electric power is supplied by public power entities that are not subject to FERC jurisdiction. For a discussion of public power, see CRS report RL31477, *Public Power and Electric Utility Restructuring*.

[99] For a discussion on a utility's legal responsibilities to provide reliable and adequate service, See, *Electricity: A New Regulatory Order?* A Report prepared by the Congressional Research Service for the use of the Committee On Energy and Commerce, U.S. House of Representatives. Committee Print 102-F. June, 1991. Pgs. 223-233.

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

[101] Further discussion of state retail competition see, CRS Issue Brief IB10006, *Electricity: The Road Toward Restructuring*.

[102] 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.

[103] President's Commission on Critical Infrastructure Protection. *"Critical Foundations: Protecting America's*
(continued...)

shelf industrial control systems, increasing the international availability of systems and their documentation. Due to the similarity between these systems and systems installed domestically, potential terrorists might not need to break into an American utility to test their plans.[104]

Another route to protect these systems is to create strong information technology protections between the exterior and interior networks, and between interior, corporate, and control system networks. This approach does not directly address industrial control system vulnerability, but rather increases the difficulties in obtaining access to them. Some experts assert that techniques for reducing the system vulnerability in such a manner are already known. They contend that the majority of attacks on industrial control systems will come through corporate networks, via the Internet. These analysts contend that if general network benchmark standards were uniformly applied across corporate networks, corporate networks vulnerability to intrusion could be reduced.[105] These benchmark standards include disabling unneeded server functionality, patching known security flaws, and updating programs to the most recent version. Historically, control system networks have been highly customized to the configuration optimal for each utility company. Because of this high degree of customization, application of patches to computer operating systems and programs must be done with great care, as unintended consequences may occur from loss of functionality. As a result, patch management and the continuing existence on control network systems of vulnerabilities with known solutions are areas where difficulties in reducing vulnerability have been highlighted.

Control system vulnerabilities unrelated to those associated with corporate networks may require more specific protection, including against attacks not crossing the corporate network.[106] Protecting corporate networks from intrusion may not address enough of the vulnerable access routes into industrial control systems to provide satisfactory degrees of protection. Some experts assert that firewalls, intrusion detection, encryption, and other technology need to be developed specifically for electric utility control systems.[107] They state that using existing information technology solutions for control system vulnerabilities will not be successful. Some security analysts contend that in addition to network security, specific protection for industrial control systems must also be established. Such protection might be addressed by successfully isolating the control system network from the corporate computer network, creating duplicates or extensive redundancy for critical control systems, or by developing and implementing stronger security measures for control systems. Such an effort might significantly increase the difficulty of infiltrating the control system network from the Internet.[108]

(...continued)

Infrastructures—The Report of the President's Commission on Critical Infrastructure Protection," United States Government Printing Office (GPO), No. 040-000-00699-1, October 1997.

[104] See, *The Clinton's Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63,* White Paper, May 22, 1998, which can be found on http://www.usdoj.gov/criminal/cybercrime/white_pr.htm. This site was last viewed by CRS on March 22, 2004.

[105] For a discussion on general critical infrastructure activities, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation.*

[106] In the 108th Congress, S. 14, S. 475, S. 1754, S. 2014, S. 2095, S. 2236, the conference report on H.R. 6, H.R. 1370, and H.R. 3004 would provide for an Electric Reliability Organization to prescribe and enforce mandatory reliability standards.

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

[108] See, http://www.esiac.com/

While most security experts agree that electric utilities that view secure industrial control systems as a priority can reduce vulnerabilities, they assert that electric utilities are not willing to voluntarily commit the necessary resources, time and effort. Stuart McClure, President and Chief Technical Officer of the security company Foundstone, contends, "[Industries] have fallen into the regulation trap. Unless the government regulates it, they're not yet taking [security] seriously."[109]

Cyber Research Activities

The federal government has not mandated cyber-security standards for electric utilities. The Federal Energy Regulatory Commission has issued a Notice of Proposed Rulemaking which includes language requiring the electric industry to self-certify that it is meeting future cyber-security standards, but no final rule has been issued.[110] Cyber-security guidelines have been developed within the electric utility sector by the North American Electric Reliability Council to provide a minimum standard for the industry, but adherence to these standards is voluntary.[111]

Research into control system security technology advances on several fronts. Encryption methods with potential application to SCADA systems are being developed by the Gas Technology Institute and the American Gas Association. The Electric Power Research Institute, through its Infrastructure Security Initiative, is developing, among other security approaches, secure communications technologies for SCADA systems. The federal government opened a public/private forum through the National Institute of Standards and Technology to develop standards for process control system requirements. The Idaho National Engineering and Environmental Laboratory, in conjunction with Sandia National Laboratories, is developing a SCADA test bed to help identify vulnerabilities and improve the security and stability of SCADA systems. Other research at the Department of Energy National Laboratories include programs at Sandia to develop secure control systems for the energy industry and the development of a Critical Infrastructure Protection Analysis Laboratory at Pacific Northwest National Laboratory which, among other things, provides an isolated network for simulating network attacks.[112]

Policy Issues

Reducing the vulnerability of the electric network to attacks has been among the more persistent security challenges facing the U.S. electric sector. There are two approaches to reducing electric infrastructure vulnerability: The first approach is to reduce the possibility of attack and the second is to speed recovery. The potential for terrorist attack has pushed the topic of reliability into the federal policy arena from its traditional venue of being an industry responsibility, subject to state regulatory authority. Beginning in the 1990s, federal policies began emerging to ensure the protection of the nation's infrastructure, including the electric system, from terrorist activities.

---

[109] 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.

[110] Another industry concern is that sharing information among utilities may raise antitrust concerns. See **Appendix B** for a legal analysis on antitrust implications of information sharing.

[111] 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.

[112] CFR 388.113(c)(2).

Originally, much of the attention was devoted to cyber-security, but also included attention to critical physical components, including transformers and transmission lines.

The primary federal role, through the Department of Homeland Security (or predecessor agencies), the Department of Energy, and other agencies, has been to characterize general vulnerabilities. For the electric system, the key vulnerabilities identified include: 1) large transformers, of which the destruction could result in regional power outages lasting for days, weeks, or even longer; 2) transmission lines, of which interruption in congested corridors could pose serious problems; and 3) cyber-systems, particularly control systems essential to generating and transmitting electricity. Identifying vulnerabilities raises questions of how to use that information and with whom to share it. Some information may be proprietary, and some could be of value to terrorists—resulting in concerns about access through the Freedom of Information Act to critical infrastructure information reported to the federal government.

A more comprehensive understanding of vulnerabilities poses the basic policy issues of:

•What should be done to address those vulnerabilities?

Most experts argue that electric utility infrastructure will always be vulnerable to attack. The issue is whether augmenting physical security, concentrating on coordination and speeding recovery efforts, or a combination of the two is the best direction.

•Who should be responsible for implementing appropriate actions?

Currently, the federal government does not require utilities (except nuclear facilities) to systematically characterize their vulnerabilities, nor are actions required to reduce vulnerabilities. A majority of state utility commissions reports that they have a 'modest' role with respect to utility security, but there is little consistency of security activities among the states. Is there a federal role to coordinate and perform vulnerability assessments that have traditionally been done by the utility industry? Additionally, should the federal government share the responsibility to reduce identified vulnerabilities?

•Who should pay?

As the utility industry moves toward competition with market-based rates rather than rates based on costs, a question arises as to who is responsible for security-related investments. Is there a role for the federal government to assume the financial liability of utility security investments or should it remain with the utilities? Should utilities that have competitive retail rates be treated the same as retail rate-regulated utilities?

•Should reliability guidelines or standards be implemented by the federal government or industry groups?

NERC has promulgated reliability guidelines for the utility industry but it has no enforcement authority. At issue is whether Congress should pass proposed Electric Reliability Organization (ERO) legislation that would allow NERC to set FERC-approved reliability standards. In addition, the proposed ERO would be given enforcement authority. Alternatively, should the federal government assume a role in developing and enforcing reliability standards for security reasons? If so, what agency would establish and enforce reliability standards (DHS, DOE, FERC)?

•Who should be responsible for carrying out research and development to reduce vulnerabilities and to improve response and recovery?

Currently, several national laboratories, the military and EPRI are conducting research and development projects to increase electric utility infrastructure protection and speed response in case of terrorist attack. Should there be a more coordinated approach to this research within the government and should there be additional coordination between industry and government activities?

These types of questions are increasingly being posed to Congress. The matter of limiting access through the Freedom of Information Act to protect sensitive infrastructure security information has been acted on (P.L. 107-296, section 214). Certain aspects of electric reliability are included in the comprehensive energy bill (H.R. 6)—notably transmission line siting and creation of an ERO—but have not been enacted. Other questions have been the subject of hearings or bills, but are unresolved or not ready for action.

Physical Security Issues

Congressional hearings identified HV transformers as a security concern 22 years ago.[113] While there appears to be widespread agreement that these transformers as well as other assets are critical and vulnerable, only limited initiatives have been taken to address the vulnerability of electric utility infrastructure. Options to reduce these vulnerabilities include: substation hardening, stockpiling spares, revitalizing domestic production of HV transformers, standardizing HV transformer design, increasing contingency planning, developing new technologies, and expanding the electricity network.

"Hardening" HV Transformer Substations

In 1989, the head of NERC testified before Congress that "doing anything to protect the transformer *per se* ... is virtually impossible."[114] While not all security experts share this view, the engineering design and operating requirements of HV transformers do make them difficult to physically reinforce ("harden") against physical attack. HV transformer substations generally incorporate basic access barriers to prevent accidents and vandalism, but not terrorism. Due to their size, transmission connections, and requirement for open-air cooling, most HV transformers cannot be completely enclosed in protective structures. Opinions vary on the incremental benefits of other access barriers and security systems, such as concrete walls, electronic locks and security alarms. The Tennessee Valley Authority (TVA), for example, found that due to regional topography and original siting requirements placing transformers in valleys rather than on hilltops, concrete barriers could not protect low-lying HV transformers against attacks from nearby hillsides or small aircraft.[115] But measures such as those in NERC's general security guidelines discussed previously could be taken in and around transformer substations to provide early indications that an attack is being planned and to make it more difficult for terrorists to

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

[114] 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.

[115] The District of Columbia and 17 states have active restructuring plans that include retail competition. An additional 5 states have delayed retail restructuring plans.

execute an attack, especially from a distance.[116] It is generally understood, however, that no measures can completely protect an HV transformer facility against determined attackers—so hardening alone is unlikely to be sufficient to dramatically reduce transformer vulnerability.

Transmission owners and the DHS appear to be emphasizing different aspects of HV transformer substation hardening. Transmission owners seem to be focusing their security efforts primarily "inside the fence" or near their HV substations in an effort to physically hamper a terrorist attack that may already be underway. The DHS supports such measures to some extent, with plans, for example, to fund access roadway barriers. But the DHS seems to be placing a greater emphasis on preventing attacks *before* they are underway—through measures such as community awareness programs, increased police patrols, and "outside the fence" surveillance. In 2003, NERC held a series of workshops for its members that emphasized these prevention measures.[117] In discussing international experience with electric infrastructure protection, for example, a DHS official recently remarked that "bigger fences may just lead to bigger bombs."[118] Accordingly, as noted earlier, DHS officials have said the Department does not intend to review the HV substation security plans of critical transformer owners. The different hardening emphases between transmission owners and DHS are not necessarily inconsistent, and may well be complementary, but they could create misunderstanding where "hardening" objectives are not clearly defined.[119]

Recovery Speed

In the event of multiple HV transformer failures, the main issue would be the time required to replace the transformers and restore reliable electric service. Several options have been proposed to speed recovery: standardizing design, maintaining a stockpile of spares, and having domestic manufacturing capability. A stockpile would be available immediately. As mentioned earlier, HV transformers take at least six months to manufacture.

Standardizing HV Transformer Design

Standardizing the designs of permanent HV transformers could facilitate emergency recovery by enabling greater interchangeability and potentially reducing unit costs. Even though many of its existing transformers are not standardized, TVA has stated that it can back up all 150 of its 500 kV units with six models of spares, including a special railcar-mounted mobile unit.[120] TVA has reduced the number of unique 500 kV transformer designs for future orders from seven to three, and has negotiated long-term agreements with two major manufacturers to supply these units.

Regional transmission organizations could assume a role in encouraging standardization by requiring transmission owners to standardize all transformer additions. Transmission owners smaller than TVA, or currently employing a wider range of HV transformer specifications, might have more difficulty employing standard designs. Coordinating such standards across utilities

[116] *Duquesne Light Co. v. Barasch*, 488 U.S. 299, 109 S.Ct. 609 (January 11, 1989). This case makes clear that prudence is an acceptable rate methodology standard among the many available to states.

[117] Federal Energy Regulatory Commission (FERC). News release. R-01-38. Washington, DC. September 14, 2001.

[118] FERC. Personal communication. October 16, 2003.

[119] McGarvey, Joe and John D. Wilhelm. NARUC/NRRI. 2003 Survey on Critical Infrastructure Security. The National Regulatory Research Institute. October 1, 2003.

[120] *Ibid.*

could be even more complicated, although it might be done with cooperative agreements. For example, BGE, PECO Energy and PSEG, which jointly developed their 500 kV transmission networks, are reported to jointly own three 500 kV transformer spares that can replace their independently-owned operating units.[121] While standardization could shorten recovery times, standard designs might also make it easier for terrorists to learn about and exploit specific engineering characteristics common to a large set of standard units.

Critical Spare Parts Stockpile

The National Research Council, NERC, and other groups have long proposed the stockpiling of spare transformers and other critical equipment as emergency replacements for critical units that do not currently have secure spares.[122] These stockpile proponents assert that, since it is difficult to completely prevent an HV transformer attack, a stockpile of critical spares is essential to minimizing the potential impacts of a widespread transformer outage. Proponents also assert that a centralized repository of spare HV transformers would greatly reduce the time to restore electric service in the event of a terrorist attack by eliminating months of manufacturing and transportation time otherwise required to build replacement units. They also assume that, given limited interchangeability, the number of transformers needed for a collective stockpile would be lower than the number utilities would need to buy individually to ensure the same level of backup for their own critical transformers. Proponents believe that a stockpile can be implemented more quickly than other HV transformer measures and involves fewer technological and regulatory uncertainties.

Specific stockpile proposals have varied, but most would identify and rank critical HV transformers in service and would compare that ranking to the nation's existing spares inventory to prioritize additional needs. A yet-to-be-designated authority would then finance the purchase of these spares and maintain them at strategically located secure locations, such as military bases, for transfer to any transmission owner facing a transformer emergency.[123] Locating critical HV transformer spares in a secure central location would be important to protect the spares themselves from attack. As noted above, DHS' National Emergency Energy Spare Parts Program seeks to implement just such a stockpile. DHS intends to develop the technology and support logistics but does not intend to purchase or maintain the stockpile itself.

Relying on existing technology, a transformer stockpile could be costly. As noted above, the nation's approximately 4,000 HV transformers are generally custom designed, so they have limited interchangeability, especially across utilities with distinct design practices. A large number of transformers deemed to be critical could therefore require many spares. DHS believes that approximately 200 to 500 HV transformers might be nationally critical, with the actual number likely nearer the low end of this range.[124] Another expert estimate also puts the number of critical HV transformers at approximately 200.[125] The cost of 200 critical transformer spares, which

---

[121] Newton, C., "The Future of Large Power Transformers." *Transmission & Distribution World*. September 1, 1997.

[122] See, CRS Report RL32075, *Electric Reliability: Options for Electric Transmission Infrastructure Improvements.*

[123] Newton, C., "The Future of Large Power Transformers." *Transmission & Distribution World*. September 1, 1997.

[124] White, Charles H. North American Electrical Manufacturers Association (NEMA). Remarks to the Senate Committee on Governmental Affairs, Hearings on Vulnerability of Telecommunications and Energy Resources to Terrorism. No. 101-73. Washington, DC. February 7, 1989. pgs. 65-67.

[125] U.S. Department of Commerce. International Trade Administration. Circular No. 8504.23. Summary of Tariffs and Taxes. Data on electrical transformers, static converters and inductors having a power handling capacity exceeding (continued...)

would probably include a high proportion of 500 kV and 750 kV units, would likely fall in the $600-900 million range, plus additional costs for building and maintaining storage facilities.[126] Spares for some of these units already exist, however, so the incremental cost of the stockpile might be lower.

Currently, there is no multi-purpose HV transformer that could adequately be used as a spare for a wide range of existing units. The near-term development of new recovery transformers adaptable for temporary use in a range of HV substations could therefore reduce the number of spares required for security. Manufacturing a set of identical recovery units might also reduce manufacturing costs and time compared to the current custom design and production process for each unit. Assuming the availability of such transformers, the OTA estimated 13 years ago that a stockpile of "important" spares might require only 80 units and might cost $130-260 million (in 2003 dollars), excluding storage costs.[127] DHS believes that, if its containerized transformer development succeeds, as few as 40 spares would be needed for a stockpile, bringing costs down to the $100-200 million range.[128] But recovery transformers are still under development and, even if the technology were developed successfully, commercial production would not happen immediately. Furthermore, since their adaptable design would significantly reduce their efficiency, recovery transformers would increase transmission requirements due to energy losses and would probably not be suitable as permanent replacements for more conventional units.[129]

EPRI and NERC are developing a database of critical spare parts owned by electric utilities.[130] In an emergency, utilities could query NERC for available spares and then initiate contact directly with the spare part owner. This would eliminate the need for utilities to have a direct replacement for all major infrastructure. However, without coordination, utilities may not maintain the number of spares necessary for quick recovery of a coordinated attack on electric utility infrastructure. At issue is who would determine for the industry what level of spares is necessary for security and reliability purposes and who would purchase the spares.

HV Transformer Manufacturing

There is currently no U.S. capability to manufacture 500 kV or larger transformers. A reliance on foreign manufacturers would increase the recovery time because of shipping. However, the additional shipping time is not significant compared to overall manufacturing time. The National Electrical Manufacturing Association (NEMA) and transformer manufacturers have suggested that producing emergency transformer replacements in the United States could be faster than importing them and might adequately meet the security needs of the transmission network. According to a Canadian manufacturer of 500 kV units, however, the absolute minimum time to

(...continued)

100,000 kVA. October 3, 2003.

[126] Personal Communication. NERC Meeting the Security Challenge Workshop. Montreal, Québec. September 18-19, 2003.

[127] NERC maintains a database of power disturbances. The database can be found at: http://www.nerc.com/~dawg/

[128] Newton, C. September 1, 1997.

[129] Loomis, William M. Strategic Partners-Technical Systems, consulting engineer. "Super-Grid Transformer Defense: Risk of Destruction and Defense Strategies." Presentation to NERC Critical Infrastructure Working Group, Lake Buena Vista, FL. December 10-11, 2001.

[130] Personal Communication. NERC Meeting the Security Challenge Workshop. Montreal, Québec. September 18-19, 2003.

manufacture a new HV transformer from an existing design is over six months. Subsequent units of the same or another existing design could be produced every two to three weeks thereafter.[131] However, even with the marginal transportation time savings of domestic supply, a six month transformer production cycle is probably too long to prevent catastrophic impacts in a widespread transformer emergency.

According to NEMA in 1989, having manufacturing capability in an emergency would be less costly than buying a large stockpile of spares.[132] Others have argued that a spare stockpile would be more economic and would lead to faster recovery of electric service. However, OTA suggested that "national security concerns may dictate the maintenance of some minimum capability even if it is not justified economically under normal conditions."[133] With diverse global manufacturing sources and the option of a stockpile, the degree of added production security from subsidizing a U.S. manufacturing capability would be questionable.

In recent years the United States' principal HV transformer suppliers have been Canada, Japan, and members of the European Union—all of which have been stable, long-term trading partners. A number of other countries, such as South Korea, Brazil, and Mexico, also sells to the United States, contributing to a global diversity in supply. Without a stockpile, domestic manufacturing capabilities might offer only modest reductions in delivery time, but they could ensure transformer availability. Domestic supplies, for example, might be less exposed to trade barriers, geopolitics, and transportation concerns that might interfere with some foreign transformer manufacturing orders.

Increasing Contingency Planning

Transmission system operators might be able to enhance their recovery capabilities through better contingency planning for coordinated HV transformer and transmission tower attacks. Again, some control systems do evaluate on an ongoing basis the potential impacts of losing several critical network nodes at once. But analyzing more than two or three simultaneous HV transformer failures is not universal practice. Simulating such failure scenarios could help identify physical and operational changes, such as reinforcing key secondary transmission facilities, that would reduce their severity. Simulations could also speed the restoration of electric service by helping to identify, in advance, major actions that would have to be taken should a major disruption occur. These actions might include dispatching electric repair crews and equipment, locating and transporting replacement transformers, establishing emergency transmission connections, and providing emergency electric service to critical users such as law enforcement and health care institutions.

Developing New Transformer Technologies

New technologies beyond EPRI's and DHS' current recovery transformer development have the potential to reduce HV transformer vulnerability. In the early 1990s, for example, Asea Brown Boveri (ABB), EPRI, and TVA collaborated on the design of transformers with new winding

[131] Pauwels Canada, Inc. Personal communication. October 20, 2003.

[132] American Electric Power (AEP).

[133] North American Reliability Council. Data available at: ftp://ftp.nerc.com/pub/sys/all_updl/docs/regional/MilesByVoltage.doc. Website last viewed by CRS on March 22, 2004.

geometries that would reduce their weight substantially. Although these units were never commercially produced due to market conditions, they were expected to be more mobile than conventional units.[134] University researchers are also beginning to develop next-generation solid-state transformers based on new semiconductor materials that could be much lighter and more efficient than current HV technology.[135] Although the research is in its very early stages, solid-state HV transformers might be extremely flexible, allowing for a wider range of operation, interchangeability, and network control. Like most new technologies, however, there is no guarantee that these kinds of HV transformer systems could be successfully developed and cost-effectively manufactured. The time-frame for deploying such technology is unknown.

Expanding Transmission Capacity

Public resistance to new transmission siting may have led transmission operators to rely on upgrades to existing transmission corridors rather than establishing new corridors. Installing HV transmission is one effective way to maximize the power transfer capability of an existing transmission corridor. HV infrastructure has allowed for increased levels of bulk power transfer between utilities that have occurred as a result of wholesale competition. The combination of electricity demand growth, increasing concentration of power flows through key transmission corridors, and increased wholesale power transactions has made regional electricity networks even more reliant on a limited set of HV transformers.[136] The more congested the transmission system, the more vulnerable the system could be to intentional attack and outages due to weather-related damage.

General expansion of U.S. transmission capacity would not prevent HV transformer or transmission tower attacks or accelerate transformer recovery. However, many experts believe that a general network expansion would alleviate the criticality of key nodes within the network—including the criticality of many HV transformers and key transmission corridors. By increasing the number and capacity of transmission interconnections and alternative transmission routes, regional power networks could more readily operate around disabled transformer stations. Operators might also have greater ability to isolate a local network area to limit the effects of a transformer disruption or transmission tower failure to the local geographic area. This approach would likely take a long time to implement, since it depends upon the resolution of wide-ranging and politically contentious barriers to new transmission investment and siting.[137] Even with more transmission, certain HV transformers would continue to be critical. By targeting a few additional transformers, for example, terrorists might still pose a substantial risk of long-term power disruptions even within an expanded transmission network.

[134] The three currents are sinusoidal functions of time but with the same frequency (60 Hertz). In a three phase system, the phases are spaced equally, offset 120 degrees from each other. With three-phase power, one of the three phases is always nearing a peak.

[135] kV=1000 volts

[136] The loss of power on the transmission system is proportional to the square of the current (flow of electricity) while the current is inversely proportional to the voltage.

[137] Transmission towers also support a fourth wire running above the other three lines. This line is intended to attract lighting, so that the flow of electricity is not disturbed.

Cyber-security Issues

SCADA system vulnerability reduction may be achieved through several routes. Advocates of enhanced general cyber-security suggest an increase in corporate and overall cyber-security, so as to limit access to critical control system networks. They suggest either voluntary or federally mandated standards for utility cyber-security. Such a method may reduce control system vulnerability by limiting the likely avenues of attack on these systems. Some have suggested that one mechanism for inducing strong cyber-security among utilities would be to require disclosure of the extent or magnitude of security efforts within a utility.

Advocates of a more targeted approach to control systems suggest several alternate solutions. One is the further implementation of best-practices within utilities to bolster the security functions already existing in control system networks. Examples of such an approach include using strong passwords on control system computers and prompt testing and implementation of vendor patches. Another remedy suggested is further public investment in security technologies specifically for control systems. Federal incentive programs for the incorporation of new security features in control system technologies is cited as a potential mechanism for increasing control system security.

An area of debate involves oversight and enforcement of security for electric utility control systems. Current oversight and guideline setting are performed by industry members and groups. Some have suggested that industry self-regulation may not provide strong enough security for these systems, and that federal agencies, such as the Federal Energy Regulatory Commission or the Department of Homeland Security, might play a regulatory role for a federal standard. The formation of an electric reliability organization as the vehicle for oversight of control system cyber-security would be another option. Standards developed by the electric reliability organization could be made enforceable and provide a potential vehicle for oversight of control system security.

A final area of potential interest lies in the development of next-generation, secure control systems, or assistance in converting current insecure systems to a more secure platform. Conversion of current control system technology to make it more secure would involve the upgrading or replacement of a significant portion of the current infrastructure. While some have suggested that add-on equipment that, for example, performed encryption/decryption would provide lower cost alternatives than replacing the control system equipment, retrofitting of current technology may be viewed by industry representatives as cost intensive.[138] Some have suggested that the normal rate of wear and replacement would serve to replace insecure components, assuming that newer, more secure components are developed, but the extended lifetime of robust control equipment implies that such an upgrading method would require a significantly long time-frame. Whether development of new secure network architecture and replacement of insecure equipment should remain areas of industry responsibility or should be mandated and/or supported by the federal government may become an issue.

[138] Platts Energy Business and Technology, Vol. 5, No. 1, January/February 2000, pg. 14.

Appendix A. High-Voltage Transformer Trade Data

Table A-1. Global High-Voltage Transformer Manufacturers, 2004

Maximum kV Class	Manufacturer	Manufacturing Locations
750	ABB Transformers	Canada (parts in Germany, Spain)
	Alstom T&D	Australia, Turkey, UK
	Ansaldo Coemsa (Finmeccanica)	Brazil
	Hyosung	South Korea
	Hitachi	Japan
	Hyundai Heavy Industries	South Korea
	Mitsubishi Electric	Japan
	Pauwels Canada	Canada
	Siemens AG	Germany
	Tamini Group	Italy
	VA TECH ELIN	Austria, Scotland
500	Bao-Ding (Toshiba)	China
	Condumex/IEM	Mexico
	Crompton Greaves Ltd.	India
	Efacec	Portugal
	ELCO Industries Ltd.	Israel
	GE-Prolec	Mexico
	Jeumont Schnieder	France
	Shenyang Transformer Works	China
	SMIT (RWE/Tessag)	Netherlands
	TM T&D (Toshiba/Mitsubishi)	Japan, Brazil, Chile
	Xi'An Electrical	China
345	Bharat Heavy Electricals Ltd.	India
	ELIN Mexico	Mexico
	NGEF Ltd.	India
	Pennsylvania Transformer	USA
	TELK	India
	Waukesha Electric Systems	USA

Source: North American Electrical Manufacturers Assoc.; Pauwels Canada; Company Web sites.

Table A-2. 2002 Export and Trade Data for High-Voltage Transfers*

Country	Exports to U.S. ($1,000s)	Mfg. Wage vs. U.S. Wage	Duty Differential with U.S.	Mfg. Wages ($/hour)	Duty on Exports to U.S.	Duty on Imports from U.S.
Canada	71,762	.77	0%	15.64	0% (NAFTA)	0% (NAFTA)
Japan	51,015	.96	-1.6%	19.59	1.6%	0%
Netherlands	26,254	.95	2.1%	19.29	1.6%	3.7%
U.K.	23,913	.79	2.1%	16.14	1.6%	3.7%
Germany	21,445	1.13	2.1%	22.86	1.6%	3.7%
Brazil	18,277	.15	14%	3.02	0%	14%
Korea	12,643	.40	6.4%	8.09	1.6%	8%
Mexico	11,853	.12	0%	2.34	0%	0% (NAFTA)
France	10,992	.78	2.1%	15.88	1.6%	3.7%
Israel	9,539	.67	0%	13.53	0%	0% (FTA)
Australia	4,399	.65	3.4%	13.15	1.6%	5%
Turkey	1,392	.05	2.1%	.94	0%	3.7%
Spain	579	.54	2.1%	10.88	1.6%	3.7%
India	0	.17	25%	3.43	0%	25%
Italy	0	.68	2.1%	13.76	1.6%	3.7%
Portugal	0	.23	2.1%	4.75	1.6%	3.7%
United States	—	1.00	0	20.32	—	—
Total	**264,063**					

Sources: U.S. Dept. of Commerce, U.S. Treasury, and U.S. International Trade Commission.

*Sales data are for transformers exceeding 100 MVA rated capacity. Duty rates calculated by CRS and are based on available data. Wages are for 2001, except 2000 for Portugal.

Appendix B. Electric Utility Infrastructure Information Sharing and Antitrust Implications

While a regular flow of infrastructure information between utilities can bolster system reliability, the practice may raise certain antitrust concerns. Exchange of certain, competitively significant information in a competitive market can lead to illegal market manipulation and can facilitate anti-competitive practices.[139] Antitrust statutes do not directly address the issue of infrastructure information sharing in the electric utility industry, and the Federal Energy Regulatory Commission has only addressed portions of the issue in its rules and policy statements.[140] Before examining the situation as it pertains to the energy industry, it is first helpful to understand the general antitrust laws and their relation to information sharing. A brief description follows.

The anti-competitive potential of information sharing has been interpreted by the courts as flowing from the general antitrust laws of the United States. Section 1 of the Sherman Act states, "[e]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several states, or with foreign nations, is declared to be illegal."[141] The Supreme Court has continuously interpreted the law to preclude only those restraints that are "unreasonably restrictive of competitive conditions," because it recognized that a literal interpretation of the broad prohibition would render every trade agreement or regulation an arguable restraint of trade.[142, 143] Accordingly, the elements of a section 1 violation are "(1) the existence of a contract, combination, or conspiracy among two or more separate entities that (2) unreasonably restrains trade and (3) affects interstate or foreign commerce."[144] In addition, there must be an intent to enter the conspiracy and an intent to effectuate the conspiracy's goals.[145]

The rule of reason typically prohibits information exchanges in industries whose structural characteristics indicate that the exchanges are likely to have anti-competitive effects.[146] The typical case in which exchange of information has been found to violate antitrust laws involves the exchange of price information, allowing the companies involved in the exchange to manipulate the markets.[147] Alternatively, exchanges are likely to be upheld if anti-competitive

---

[139] Personal communication with industry official, September 18, 2003.

[140] U.S.C. 791a et seq.

[141] U.S.C. 824(b)(1). Under FERC Order 888, FERC asserts jurisdiction over transmission used for wholesale transactions as well as over transmission in states where the transmission services and electricity are sold separately at retail, so called "unbundled" retail sales. In New York et al. v. Federal Energy Regulatory Commission, 535 U.S. 1 (2002), the U.S. Supreme Court held that FERC has jurisdiction over transmission including unbundled retail transactions.

[142] Nebraska electric power is supplied by public power entities that are not subject to FERC jurisdiction. For a discussion of public power, see CRS report RL31477, *Public Power and Electric Utility Restructuring*.

[143] For a discussion on a utility's legal responsibilities to provide reliable and adequate service, See, *Electricity: A New Regulatory Order?* A Report prepared by the Congressional Research Service for the use of the Committee On Energy and Commerce, U.S. House of Representatives. Committee Print 102-F. June, 1991. Pgs. 223-233.

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

[145] Further discussion of state retail competition see, CRS Issue Brief IB10006, *Electricity: The Road Toward Restructuring*.

[146] 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.

[147] President's Commission on Critical Infrastructure Protection. *"Critical Foundations: Protecting America's Infrastructures—The Report of the President's Commission on Critical Infrastructure Protection*," United States
(continued...)

effects are unlikely or outweighed by legitimate business reasons.[148] It is important to note that not every exchange of price information is an automatic violation of antitrust law, nor will exchanges of other types of information (e.g., costs, infrastructure) necessarily fall within legal parameters.[149] The deciding factor is whether the information is competitively significant.[150]

FERC has seldom addressed information exchanges between utilities, especially from an antitrust perspective. Where it has addressed infrastructure information, FERC has dealt with protecting critical infrastructure information from falling into the wrong hands, i.e. terrorists'.[151] In policy more related to traditional antitrust concerns, FERC has prohibited certain types of information sharing between transmission providers and those responsible for "wholesale merchant functions,"[152] but in the comments to a recently published final rule, FERC at least indirectly supported such infrastructure information sharing through NERC. In its explanation of section 13.1's new confidentiality provisions for reliability purposes,[153] FERC stated:

> the Final Rule must allow information to be shared with Transmission Provider representatives of NERC and other regional planning groups, since to deny them this information may undermine Transmission System reliability and modeling efforts. Section 13.1 of the Final Rule allows the Parties to share Confidential Information with an independent transmission administrator or reliability organization as long as the disclosing party agrees to promptly notify the other Party in writing and to seek to protect the Confidential Information from public disclosure. . . .[154]

The final rule and accompanying comments do not address antitrust concerns directly.

NERC, the organization that now facilitates inter-utility information exchange, has based the structure of its information sharing system, at least in part, on antitrust considerations, using various means to insulate sensitive exchanges from antitrust review.[155] Apart from its own services, NERC has offered no official position on the limits of information exchange nor does it have the authority to do so definitively. The most explicit direct application of antitrust principles to utility information exchange thus far promulgated has been the Department of Justice's

(...continued)

Government Printing Office (GPO), No. 040-000-00699-1, October 1997.

[148] See, *The Clinton's Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63,* White Paper, May 22, 1998, which can be found on http://www.usdoj.gov/criminal/cybercrime/white_pr.htm. This site was last viewed by CRS on March 22, 2004.

[149] For a discussion on general critical infrastructure activities, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation.*

[150] In the 108th Congress, S. 14, S. 475, S. 1754, S. 2014, S. 2095, S. 2236, the conference report on H.R. 6, H.R. 1370, and H.R. 3004 would provide for an Electric Reliability Organization to prescribe and enforce mandatory reliability standards.

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

[152] See, http://www.esiac.com/

[153] 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.

[154] Another industry concern is that sharing information among utilities may raise antitrust concerns. See **Appendix B** for a legal analysis on antitrust implications of information sharing.

[155] 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.

(DOJ's) favorable business review of EPRI's Enterprise Infrastructure Security program.[156] The business review does not, however, provide extensive guidelines for compliance with antitrust laws beyond participation in this particular program.[157]

These varied and primarily indirect positions regarding antitrust implications of utility infrastructure information exchange do little to clarify legal boundaries. Without industry specific guidelines from DOJ or FERC, legal authority for the determination of anti-competitive information sharing schemes is left to the somewhat relativistic "rule of reason" standard. This standard is inherently fact-specific and provides few firm guidelines that utilities can themselves apply. General courts will look to the following factors, many of them enunciated in cases not addressing information sharing at all, or sharing of price information only, in analyzing an information exchange under the rule of reason:

1. Whether the structure of the market and nature of the information exchanged indicate a likelihood the conduct in question will have anti-competitive effects;[158]
2. Whether the structure of the market leaves it "susceptible to the exercise of market power through tacit coordination;"[159]
3. Whether there have been adverse effects on consumer welfare;[160]
4. Whether the anti-competitive effect outweighs the beneficial effects of the information sharing;[161]
5. And whether there was an implicit or explicit agreement to engage in unlawful conduct associated with the information exchange, such as price-fixing.[162]

While the above-mentioned factors are neither easily applied nor exhaustive, they do serve to illustrate that information sharing is not always a violation of the antitrust law and that antitrust sanctions are not automatic, absent an illegal intent to suppress competition, or an actual suppression of competition in the absence of some overriding justification.[163]

[156] 18 CFR 388.113(c)(2).

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

[158] 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.

[159] The District of Columbia and 17 states have active restructuring plans that include retail competition. An additional 5 states have delayed retail restructuring plans.

[160] *Duquesne Light Co. v. Barasch*, 488 U.S. 299, 109 S.Ct. 609 (January 11, 1989). This case makes clear that prudence is an acceptable rate methodology standard among the many available to states.

[161] Federal Energy Regulatory Commission (FERC). News release. R-01-38. Washington, DC. September 14, 2001.

[162] FERC. Personal communication. October 16, 2003.

[163] This section of this report was written by former CRS Legislative Attorney Aaron Flynn.

Author Contact Information

Amy Abel
Section Research Manager
aabel@crs.loc.gov, 7-7239

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy
pparfomak@crs.loc.gov, 7-0030

Dana A. Shea
Specialist in Science and Technology Policy
dshea@crs.loc.gov, 7-6844