Pulling the Plug on the Nation´s Power Grid:

Cyberthreats and Homeland Security Challenges

By David Z. Bodenheimer

> We shouldn’t have to wait for the cyber equivalent of a Hurricane Katrina . . . to realize that we are inadequately prepared to prevent, detect and respond to cyber attacks. And a cyber attack can affect a far larger area at a single stroke than can any hurricane. Not only that, given the increasing reliance of critical infrastructures on the Internet, a cyber attack could result in deaths as well as in massive disruption to the economy and daily life. (Rep. Boehlert, Sept. 2005.)[1]

With continuing vigor, Congress, industry, and others have voiced strong concerns about the vulnerability of America’s critical infrastructure to crippling attacks by cyberterrorists. Such “digital Pearl Harbor” attacks do not lack for potential targets, as the information technology revolution has interwoven cyberdependence into everything from financial and telecommunication networks to sewage processing and flood control.

Nowhere is the debate more charged—and the risk more starkly apparent—than the nation’s electrical power grid. The forces of deregulation and competition have produced a highly interconnected electric power sector now heavily dependent on real-time information, remote control, and data monitoring via phone lines, wireless links, and the Internet. Although such trends have boosted productivity, they have also multiplied the number of portals through which hackers and cyberterrorists may sneak in and work their mischief. At the same time, the interconnected power grid heightens the risk that a single-point failure—whether caused by falling trees or hackers’ keystrokes—may trigger an electric avalanche much like the massive blackouts shrouding the Northeast in August 2003 and the Northwest in August 1996.

Recent congressional, federal, and industry initiatives all have recognized the threat and taken steps to plug the gaps. This article will focus upon the nature of the threat from cyberattacks, the responsibilities for addressing these threats, and the opportunities for further improvements.

The Cyberthreat to the Nation’s Power Grid

As the National Research Council warned, “Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb.”[2] The specter of cybercriminals or terrorists reaching through the Internet and wreaking havoc on dams, sewage treatment facilities, electric power plants, or other critical infrastructures has been described as a “digital Pearl Harbor.” While some have discounted this risk,[3] a survey of corporate chief security officers found that 45 percent expect such an attack eventually, with 13 percent anticipating such an attack within the year.[4] Such concerns have ample foundation, as vulnerabilities have continued to surface, hackers have acquired greater skill and sophistication, and cybercrime has risen since 1997 by 3,600 percent.[5]

The Power Grid as a Cybertarget

The North American power grid is an enormous engineering marvel—nearly 3,500 utility organizations with more than $1 trillion of infrastructure assets deliver electricity over more than 200,000 miles of transmission lines to 283 million people.[6] To manage the geographically far-flung and remote power facilities, the industry depends upon supervisory control and data acquisition (SCADA) systems for centralized control and monitoring of the information.[7] Since deregulation, the electric power industry’s escalating demand for real-time information and automated controls has driven its growing dependence upon a host of

Bodenheimer (dbodenheimer@crowell.com) is a partner in the Washington, DC, office of Crowell & Moring LLP (www.crowell.com) where he specializes in government contracts and homeland security. He currently serves as Vice Chair on the ABA Section of Science & Technology Law’s Special Committee on Homeland Security. He thanks cocommittee member Steven Roberts for his keen insights and comments.

information technologies, including local and wide area networks, Internet, wireless networks, satellite connections, and radio links.[8] With these market forces and industry trends have come with a number of changes that magnify the risk and potential damage flowing from cyberassaults on the power grid:

- The shift away from proprietary solutions to standardized technologies (e.g., Microsoft Windows and Unix-like operating systems) with known vulnerabilities
- The increased connectivity of control systems to other networks
- The rapid and widespread distribution of technical information about control systems.[9]

Ironically, the very changes that have boosted the industry's productivity and efficiency have also eroded the power grid's defenses against cyberthreats.

The risk is real. Indeed, translations of Al Qaeda documents from 2002 identified the electric power grid as a cybertarget of interest.[10] In an interview, the cochairman of the President's Information Technology Advisory Committee (PITAC) stated: "If you wanted to go after the electric power grid—even the physical elements of the electric power grid—then a cyberattack would surely be the most effective method."[11] Based upon interviews with representatives of the power industry, a task force for the National Security Telecommunications Advisory Committee concluded that a "well-supported terrorist group" could "conduct a structured attack on the electric power grid electronically, with a high degree of anonymity, and without having to set foot in the target nation."[12]

The Incidence of Cyberattacks

The cyberattacks have been persistent. For example, a Baltimore power company acknowledged that hackers attempt to penetrate the computer network "[h]undreds of times a day."[13] According to the National Research Council, "security experts reported that 70 percent of energy and power companies experience at least one severe cyberattack."[14] Nearly all of the attacks have failed, but some of the attacks have cracked the security perimeter of the power grid, such as when "the Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant and disabled a safety monitoring system for nearly five hours."[15] GAO summed up such attacks as follows:

> In March 2005, security consultants within the electric industry reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities' electronic control systems. Computer security specialists reported that, in a few cases, these intrusions had "caused an impact." While officials stated that hackers had not caused serious damage to the systems that feed the nation's power grid, the constant threat of intrusion has heightened concerns that electric companies may not have adequately fortified their defenses against a potential catastrophic strike.[16]

A variety of simulated cyberattacks has confirmed the vulnerability of the power grid. After officials at the Energy's Department's Idaho National Laboratory demonstrated how a skilled hacker could cause serious damage, the chairman of the Federal Energy Regulatory Commission (FERC) described his reaction by saying "I wish I'd had a diaper on."[17] Similarly, Richard Clarke (former head of federal cybersecurity) stated: "Every time the government has tested the security of the electric power industry, we've been able to hack our way in—sometimes through an obscure route like the billing system."[18] In one unsettling example, a research manager at the British Columbia Institute of Technology explained how to use free software (like AirSnort and NetStumbler) and a Pringles can (as an antenna) to breach security of a wireless system at a remote power facility.[19] In short, these incidents and exercises confirm that if the castle doors are not already open, they are straining—and perhaps ready to crack—under the steady battering of cyberattacks.

The Risk of Catastrophic Damage

If hackers or terrorists do break through the cyberdefenses, such an attack could play hell with the power grid. The August 2003 blackout, although not caused by terrorists, illustrates the potential devastation. This blackout ripped through the power grid in the Northeast and Canada, leaving 50 million people without power.[20] In its wake, this blackout left between $7 billion and $10 billion in economic damage.[21] With a cyberattack, terrorists could wreak comparable havoc:

> In the wake of the August 2003 blackout, many experts pointed out that even if terrorism had no role in that particular incident, terrorists could easily target the power grid with similarly spectacular results at some future time.[22]

Although some dispute exists about whether anyone would die in a cyberattack,[23] such predictions do exist, with some casualty estimates ranging into the "thousands" on a scale comparable to the Bhopal industrial accident in India.[24] Patients in hospitals would be particularly vulnerable, because even though such facilities generally have independent power generators,[25] serious questions remain about such generators due to erratic maintenance, past failures, and the ability to outlast a major power outage.[26]

The most likely—and also most devastating—scenario would involve an attack during an August heat wave in the southern states such as Florida or Arizona with substantial retirement communities. During such periods of high utilization, the power grid lacks the excess capacity to absorb the rerouted power from a failed transmission path, leading to a cascading series of failures similar to the August 2003 blackout.[27] The French heat wave in August 2003 illustrates the deadly consequences to the elderly when extreme heat combines with no air conditioning. During the first week, more than 3,000 people died in France alone, with the number rising to more than 14,000 during the month of August.[28] As this incident demonstrates, even short periods without electricity to power air conditioning can have serious, even deadly, effects upon the elderly population.

Private industry is reluctant to share confidential, critical information with DHS due to a lack of confidence that such information will be properly protected.

The Responsibility for Combating Cyberterrorism

The huge cybersecurity job is spread among many players. For the electrical sector, the key responsibilities fall upon the Department of Homeland Security (DHS), the Department of Energy (DOE), and industry.

The Homeland Security Department as the "Focal Point"

Since its inception, DHS has been tasked with cybersecurity as a key mission. As required by the Homeland Security Act of 2002 (Pub. L. No. 107-296, § 201(d)), these responsibilities include assessing threats and vulnerabilities, preparing a national plan for protection, accessing and disseminating information, and securing "communications and information technology infrastructure." Senator Coburn summed the job up crisply: "The Act requires DHS to 1) assess our vulnerability to cyber attack, 2) develop a plan to fix it, and 3) implement that plan using measurable goals and milestones."[29] Accordingly, DHS serves as "a focal point for the security of cyberspace."[30]

DHS has also been a lightning rod for criticism. For example, Senator Akaka complained of "the failure by DHS to complete a comprehensive cyber threat and vulnerability assessment."[31] The Presidential Directive called for such a plan by 2004, but the plan remains in draft as DHS seeks comments.[32] In a report in July 2005, GAO identified DHS's thirteen "Key Cybersecurity Responsibilities," but found that DHS had fallen short in all thirteen areas because plans and assessments "are not yet complete," tools for cyberanalysis were "not yet developed," and other tasks remained undone or incomplete.[33] This report identified numerous causes for these shortcomings, such as:

- *Organizational Stability*: "multiple senior DHS cyber officials . . . have left the department";
- *Organizational Authority*: "officials lack the authority to represent and commit DHS to efforts with the private sector";
- *Hiring and Contracting*: "NCSD [National Cyber Security Division] is hampered by how long it takes to award a contract"; and
- *Information Sharing*: "effective communications are not yet in place in support of our nation's cybersecurity."[34]

Based upon these findings, GAO concluded that until DHS "begins to address these underlying challenges, DHS cannot achieve significant results in coordinating cybersecurity activities."[35]

Recognizing these challenges, DHS Secretary Chertoff has taken promising steps by creating a new office to be headed by the assistant secretary for cyber security.[36] With higher level attention, DHS should be better positioned to grapple with the cybersecurity challenges highlighted by Congress, GAO, and others.

The Role of the Department of Energy

Although DHS serves as the cybersecurity focal point, DOE has specific responsibility for the energy sector, "including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities."[37] The recent Energy Policy Act of 2005 (Pub. L. No. 109-58) fortifies DOE's responsibilities for cybersecurity in the electric power industry. As part of this Act, Congress included the Electricity Modernization Act of 2005 (Pub. L. No. 109-58, Title XII) that establishes the framework for developing mandatory and enforceable reliability standards to govern much of the electric power industry. Such mandatory reliability standards represented the foremost recommendation of the U.S.-Canada Power System Outage Task Force in the aftermath of the August 2003 blackout.[38]

Under this Act, FERC has the jurisdiction for both approval and enforcement of the reliability standards. Such reliability standards include "cybersecurity protection" to ensure reliable operation "so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."[39] As part of this effort, FERC must certify an "Electric Reliability Organization" that will establish and enforce the reliability standards, subject to FERC review.[40]

To implement this statutory requirement, FERC issued proposed rules on September 7, 2005.[41] Comments have been filed by interested parties such as the North American Electric Reliability Council (NERC).[42] A number of issues remain to be worked out, including the mechanism for international cooperation with Mexico and Canada, the types of reliability standards to be developed, and the nature of sanctions for noncompliance. However, because the reliability standards will be mandatory, internal corporate auditors are already considering how to monitor compliance within their organizations.[43]

The Role of Industry

With 85 percent of the critical infrastructure in the hands of the private sector,[44] much of the burden of cybersecurity has been shouldered by businesses and industry associations. In August 2003, NERC issued a voluntary industry standard known as Urgent Action Cyber Security Standard 1200.[45] By 2005, most of the major utilities and independent system operators "are darn near fully compliant with 1200."[46] However, this standard has a rather limited scope, as it specifically exempts substations, power plants, and remotely operated control systems.[47]

A more comprehensive set of NERC cybersecurity standards (CIP-002-1 to CIP-009-1) have been published in draft with proposed implementation targeted to begin in 2006, assuming approval milestones can be met.[48] These proposed industry standards may become a source for the mandatory reliability standards to be developed and approved under the Electricity Modernization Act (Pub. L. No. 109-58, § 1211).[49]

Nonetheless, the electric industry faces a number of operational, financial, and structural challenges in attempting to accelerate the pace of implementing cybersecurity standards. Unlike many sectors, the electric power industry cannot readily flip the off switch and shut a control system down to install new security upgrades or patches: "unlike typical IT networks, systems in process-control environments go months, even years, without being rebooted."[50] In addition, much of the industry is populated with older "legacy" equipment, such as communications gear for SCADA controls that can last 30 years or more.[51] Although such equipment may be more susceptible to cyberattacks,[52] replacement of the equipment can be cost-prohibitive and thus may well require approval of rate hikes by public utility commissions.[53] Finally, the power industry has been characterized by long project definition and delivery cycles that (when combined with limited investment resources for maintenance and upgrades) result in the energy SCADA infrastructure lagging behind that of the general information technology infrastructure.[54] In short, the cybersecurity fixes to the electric power industry will be neither quick nor inexpensive.

The Cybersecurity Challenges for the Power Grid

Federal agencies, Congress, and industry all have a steep climb ahead on the way to cybersecurity. Of the many challenges impeding such progress, two stand out as areas where real improvement can—and should—be made.

Long-Range Research and Development

Hardly anyone challenges the essential need for cyberresearch and development.[55] This demand is driven by multiple factors. In some areas, the needed technology simply does not exist, thus requiring a new cyberinnovation to fill the need.[56] In other areas, cybertechnology is available, but not cost-effective.[57] In any event, the cybercriminals are getting faster, smarter, and sneakier, as "the sophistication and effectiveness of cyberattacks have steadily advanced."[58] At one time, hackers needed months or even years to write code to take advantage of a vulnerability or flaw in an operating system or application; today, the average window for seizing upon such weaknesses is 5.8 days.[59] Thus, more funding is needed for the defenders to win the cyberarms race against the attackers.

Research to fortify the power grid's cybersecurity is plowing ahead at a number of facilities, such as Idaho National Laboratory and University of Illinois' Trustworthy Cyber Infrastructure for the Power Grid.[60] Unfortunately, the DHS funding for cybersecurity research and development actually dropped from $18 million in fiscal year (FY) 2005 to $16.7 million in FY 2006.[61] Furthermore, the cyberpriorities have increasingly shifted toward short-term, immediate-application research and away from long-term research that offers the potential for major scientific breakthroughs.[62] As the President's Information Technology Advisory Committee recommended, cybersecurity research and development needs additional funding, with a greater share to be focused upon fundamental, long-term research.[63]

Information Sharing and Security

Information sharing represents a fundamental reason for DHS's existence: "This information sharing is critical to successfully addressing increasing threats and fulfilling the mission of DHS."[64] Likewise, information security is crucial to the DHS mission.[65]

Unfortunately, private industry is reluctant to share confidential, critical information with DHS due to a lack of confidence that such information will be properly protected. In a July 2005 report, GAO described broad concerns cutting across industry sectors:

> Representatives from critical infrastructure sectors stated that entities within their respective sectors still do not openly share cybersecurity information with DHS. As we have reported in the past, much of the concern is that the potential release of sensitive information could increase the threat to an entity. In addition, sector representatives stated that when information is shared, it is not clear whether the information will be shared with other entities—such as other federal entities, state and local entities, law enforcement, or various regulators—and how it will be used or protected from disclosure.[66]

The same concerns exist within the electric power industry.[67] Such worries within the industry have real foundation, given that DHS—the "focal point for cybersecurity"—received an F on its cybersecurity report card.[68]

In order to perform its mission and

complete the cybersecurity infrastructure threat and vulnerability assessments, DHS must win the confidence of both industry and Congress. One positive step would be to meet the information security requirements established by the Federal Information Security Management Act of 2002 (FISMA) (Pub. L. No. 107-347, Title III), so that DHS could earn a passing cybersecurity grade next year. Another step would be to gather comments from industry and structure an information security program that specifically addresses industry concerns about cybersecurity. With such measures in place, DHS would be better positioned to fulfill its role as the "focal point" for defending cybersecurity.

Conclusion

In the cyberwars, the initial battle demands awareness and recognition at all levels—government, industry, and the general public—that the cyberthreat to the power grid is both real and potentially catastrophic. This alarm has been loudly and frequently sounded in congressional hearings, GAO reports, presidential and executive task forces, and ubiquitous news releases. The next battle requires action in response to the threat to the power grid. Many promising actions have occurred in 2005, including DHS's creation of an office of the assistant secretary for cyber security, Congress's passage of the Electricity Modernization Act, and industry's preparation of a new draft of comprehensive cybersecurity standards for the electric power sector. The final battle exists only in the imagination of some science fiction writer, as the cyberwar has no prospect of ending. Cybersecurity will be a grueling, expensive, continuous fight—but it beats the alternative. ◆

Endnotes

1. *Cybersecurity: U.S. Vulnerability and Preparedness: Hearings Before the House Comm. on Science*, 109th Cong. (Sept. 15, 2005).

2. *Cybersecurity for the Homeland: Report of the Chairman and Ranking Member of the House Subcomm. on Cybersecurity, Science, and Research & Development of the Select Comm. on Homeland Security 9* (Dec. 2004) [hereinafter "2004 House Cybersecurity Report].

3. Clark, *Computer security officials discount chances of "digital Pearl Harbor,"* GovExec.Com Daily Briefing (June 3, 2003).

4. UPI, *CSOs Worry About Digital Pearl Harbor,* Newsfactor Network (July 22, 2005) (www.newsfactor.com).

5. 2004 House Cybersecurity Report at 11; Government Accountability Office (GAO), *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity* 3–5 (July 2005) (GAO-05-827T).

6. U.S.-Canada Power Systems Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations 5 (Apr. 2004) [hereinafter "Final Report on August 2003 Blackout].

7. Sevounts, *Cybersecurity Threats and the Power Grid*, 8 World Energy 141 (2005); Final Report on August 2003 Blackout at 133.

8. Sevounts, *Cybersecurity Threats and the Power Grid*, 8 World Energy 142 (2005); GAO, Technology Assessment: Cybersecurity for Critical Infrastructure Protection 40 (May 2004) (GAO-04-321).

9. GAO, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems* 12–14 (Mar. 2004) (GAO-04-354); GAO, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection* 36 (May 2004) (GAO-04-321); GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity* 17 (July 2005) (GAO-05-827T); Sevounts, *Cybersecurity Threats and the Power Grid*, 8 World Energy 142 (2005).

10. Blum, *Hackers Target U.S. Power Grid,* Washintonpost.com E1 (Mar. 11, 2005); *see also* Gallman, *Cyber-Attacks by Al Qaeda Feared,* Washintonpost.com A1 (June 27, 2002) (browser data and interrogations revealed Al Qaeda interest in control systems for critical infrastructure).

11. Worthen, *Security: The Sky Really Is Falling,* CIO Mag. (Oct. 1, 2005).

12. GAO, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems* 14 (Mar. 2004) (GAO-04-354).

13. Blum, *Hackers Target U.S. Power Grid,* Washingtonpost.com E1 (Mar. 11, 2005).

14. GAO, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems* 12 (Mar. 2004) (GAO-04-354).

15. Poulsen, *Sluggish movement on power grid cyber security,* The Register (Aug. 16, 2004); *see also* Final Report on August 2003 Blackout at 133.

16. GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity* 4 (July 2005) (GAO-05-827T).

17. Blum, *Hackers Target U.S. Power Grid,* Washingtonpost.com E1 (Mar. 11, 2005).

18. Hoopes, *New focus on cyber-terrorism,* Christian Sci. Monitor (Aug. 16, 2005).

19. Arabe, *U.S. Power Grid Vulnerable to Cyberattacks,* Ind. Market Trends (Jan. 17, 2003).

20. Hand, *Center is planned to improve security of national power grid*, STLtoday.com (Aug. 16, 2005); Final Report on August 2003 Blackout at 1.

21. GAO, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection* 34 (May 2004) (GAO-04-321); *see also* 2004 House Cybersecurity Report at 12-13 (economic impact estimated at $6-10 billion).

22. GAO, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection* 35 (May 2004) (GAO-04-321).

23. Lemos, *Safety: Assessing the infrastructure risk,* C/Net News.Com (Aug. 26, 2002) (http://news.com/2009-1001_3-954780.html) (Michael Vatis, former director of the National Infrastructure Protection Center, stated that "It would be hard to kill people or have a lasting effect using cyberattacks").

24. *Cybersecurity: U.S. Vulnerability and Preparedness: Hearings Before the House Comm. on Science,* 109th Cong. (Sept. 15, 2005) (statement of Rep. Boehlert); Hoopes, New focus on cyber-terrorism, Christian Sci. Monitor (Aug. 16, 2005) (cyberattack on a utility or chemical plant "could kill not just workers at the plant, but thousands of civilians in the surrounding area").

25. Lemos, *Safety: Assessing the infrastructure risk,* C/Net News.Com (Aug. 26, 2002) (http://news.com/2009-1001_3-954780.html).

26. *Critical Infrastructure: Healthcare IT's perfect storm?* Healthcare Informatics Online (Nov. 2003).

27. Schintler, Kulkarni, Gorman, & Stough, *Power and Packets: A Spatial Network Comparison of the US Electric Power Grid and Internet Network,* The Critical Infrastructure Protection Program: Workshop II Working Papers 29 (George Mason Univ. Press 2004).

28. *French heat toll tops 11,000,* CNN.com (Aug. 29, 2003); *France heat wave death toll set at 14,802,* USA Today (Sept. 25, 2003); Mardy, *French heatwave disaster of August 2003,* Everything2.com (June 4, 2004) (www.everthing2.com).

29. Securing Cyberspace: Efforts to Protect National Information Infrastructures Continue to Face Challenges: Hearings Before the Senate Comm. on Homeland Security and Governmental Affairs, 109th Cong. (July 19, 2005).

30. Homeland Security Presidential Directive (HSPD) No. 7, § 16 (Nov. 17, 2003) (www.whitehouse.gov/news/releases/2003/12/20031217-5.html).

31. *Securing Cyberspace: Efforts to Protect National Information Infrastructures Continue to Face Challenges: Hearings Before the Senate Comm. on Homeland Security and Governmental Affairs,* 109th Cong. (July 19, 2005).

32. HSPD 7, § 27 ("the Secretary shall produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection . . . within 1 year from the issuance of this directive"); 70 Fed. Reg. 66,840 (Nov. 3, 2005) (seeking comments on "draft National Infrastructure Plan").

33. GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity* 9–10 (July 2005) (GAO-05-827T).

34. *Id.* at 11–14.

35. *Id.* at 15.

36. *Cybersecurity: U.S. Vulnerability and Preparedness: Hearings Before the House Comm. on Science,* 109th Cong. (Sept. 15, 2005) (statement of Mr. Purdy, Acting Director, NCSD).

37. HSPD No. 7, § 18(d).

38. Final Report on August 2003 Blackout at 2–3.

39. Pub. L. No. 109-58, § 1211, 119 Stat. 941–42 (2005).

40. *Id.*

41. 70 Fed. Reg. 53,117–33 (Sept. 7, 2005).

42. Vancko, *NERC Commends FERC's Proposed Electric Reliability Organization Rule* (Oct. 7, 2005) (www.nerc.com/~filez/nerc_filings_ferc.html.)

43. Filipek, *New Law Tightens Cybersecurity in U.S. Power Companies,* 8 ITAudit (Oct. 15, 2005) (www.theiia.org).

44. *Cybersecurity: U.S. Vulnerability and Preparedness: Hearings Before the House Comm. on Science,* 109th Cong. (Sept. 15, 2005) (statement of Mr. Donald Purdy, Acting Director, NCSD).

45. NERC Reliability Standards (https://standards.nerc.net/).

46. Hoffman, *New energy bill has cybersecurity repercussions,* Computerworld (Aug. 11, 2005) (quoting Laurence Brown of Edison Electric Institute, Inc.) (www.computerworld.com).

47. Poulsen, *Sluggish movement on power grid cybersecurity,* The Register (Aug. 16, 2004).

48. Filipek, *New Law Tightens Cybersecurity in U.S. Power Companies,* 8 ITAudit (Oct. 15, 2005) (www.theiia.org); NERC Reliability Standards (https://standards.nerc.net/).

49. *Id.*

50. Sevounts, *Cybersecurity Threats and the Power Grid,* 8 World Energy 141 (2005).

51. *Securing Cyberspace: Efforts to Protect National Information Infrastructures Continue to Face Challenges: Hearings Before the Senate Comm. on Homeland Security and Governmental Affairs,* 109th Cong. (July 19, 2005) (statement of Paul Skare, Product Manager, Siemens Power).

52. Blum, *Hackers Target U.S. Power Grid,* Washingtonpost.com E1 (Mar. 11, 2005).

53. *Securing Cyberspace: Efforts to Protect National Information Infrastructures Continue to Face Challenges: Hearings Before the Senate Comm. on Homeland Security and Governmental Affairs,* 109th Cong. (July 19, 2005) (statement of Paul Skare, Product Manager, Siemens Power).

54. *Id.*

55. "Cyber-related research and development (R&D) is vital to improving the resiliency of the Nation's critical infrastructure." *Cybersecurity: U.S. Vulnerability and Preparedness: Hearings Before the House Comm. on Science,* 109th Cong. (Sept. 15, 2005) (statement of Mr. Donald Purdy, Acting Director, NCSD).

56. Poulsen, *Sluggish movement on power grid cybersecurity,* The Register (Aug. 16, 2004) (quoting Lou Leffler, NERC cyber security chief).

57. *Id.*

58. GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity* 3 (July 2005) (GAO-05-827T).

59. Sevounts, *Cybersecurity Threats and the Power Grid,* 8 World Energy 141 (2005).

60. DOE, Idaho National Laboratory, Energy Security (www.inl.gov/nationalsecurity/energysecurity/index.shtml); Hand, *Center is planned to improve security of national power grid,* STLtoday.com (Aug. 16, 2005).

61. Hoover, *Homeland Security Funds Advanced Cyber-Security Projects,* InformationWeek (Nov. 8, 2005) (www.informationweek.com).

62. Worthen, *Security: The Sky Really Is Falling,* CIO Magazine (Oct. 1, 2005); *The Future of Computer Science Research in the U.S.: Hearings Before the House Science Comm.,* 109th Cong. (May 12, 2005) (statement of William Wulf, President, National Academy of Engineering).

63. PITAC, Cyber Security: A Crisis of Prioritization 2–4 (Feb. 2005).

64. GAO, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues* 12 (Sept. 17, 2003) (GAO-03-1165T); *see also* Pub. L. No. 107-296, § 201(d)(9).

65. Pub. L. No. 107-296, § 201(d)(12) (ensure that information "is protected from unauthorized disclosure") and § 214(a)(1) (protect critical infrastructure information from disclosure); HSPD No. 7 § 10 ("Federal departments and agencies will appropriately protect information associated with carrying out this directive").

66. GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity* 14 (July 2005) (GAO-05-827T).

67. *Cybersecurity: U.S. Vulnerability and Preparedness: Hearings Before the House Comm. on Science,* 109th Cong. (Sept. 15, 2005) (statement of Gerald Freese, Enterprise Information Security Director, American Electric Power).

68. *Davis Statement on 2004 Federal Computer Security Report Card Grades,* House Government Reform Comm. (Feb. 16, 2005) (http://reform.house.gov/GovReform/News/DocumentSingle.aspx?DocumentID=22247).