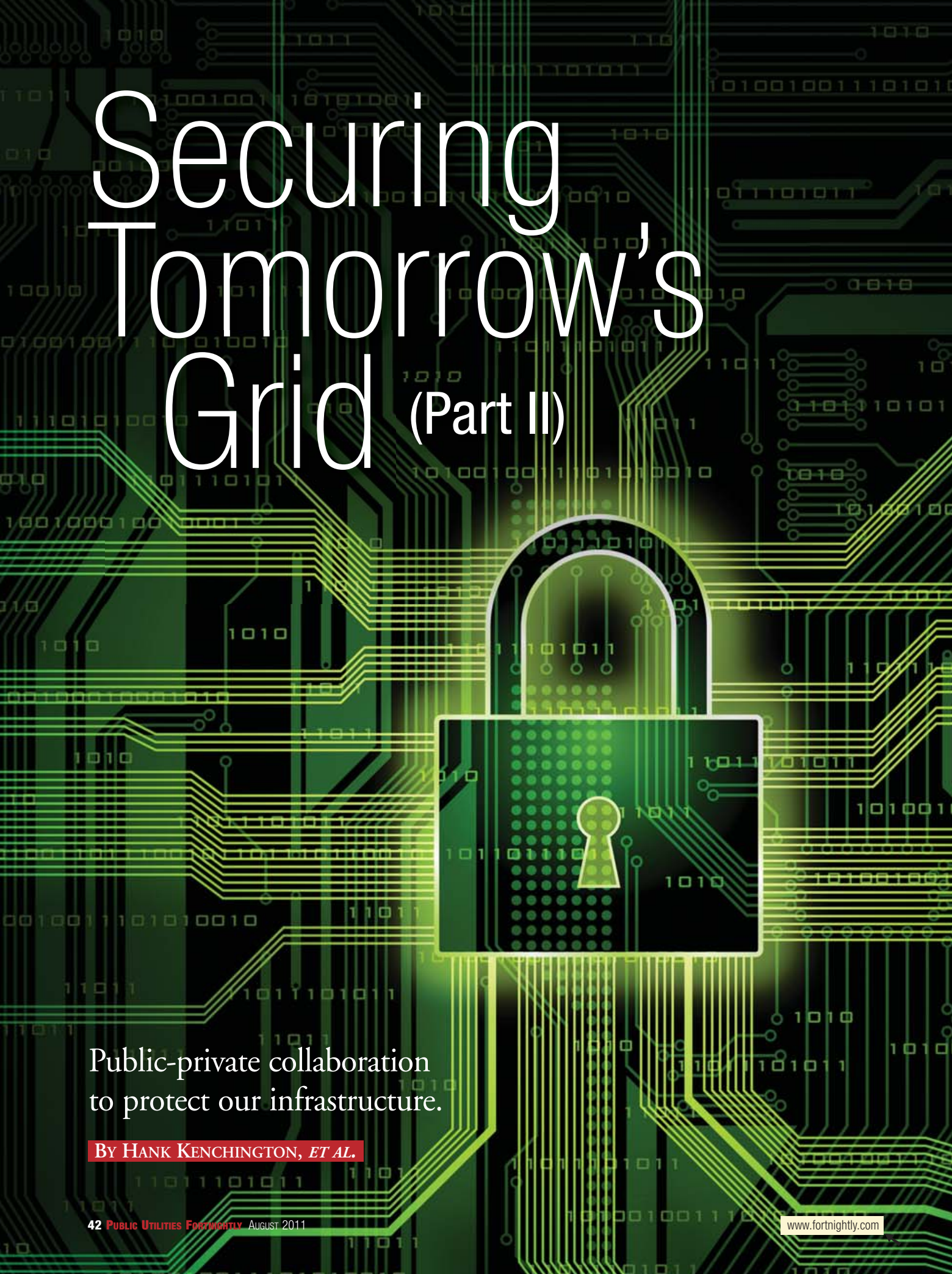
Securing Tomorrow's Grid (Part II)



Public-private collaboration to protect our infrastructure.

By Hank Kenchington, *et al.*

Intelligent systems and two-way communications are bringing a host of advancements to the utility industry, from time-of-use metering to faster outage detection and service restoration. But this smart grid also presents new cyber security challenges, as malicious actors and malware threaten customer privacy and grid operations.

The utility industry faces threats in several operational domains, such as transmission, distribution and home area networks *(see "Securing Tomorrow's Grid (Part I)," Public Utilities Fortnightly, July 2011)*. Securing these domains to manage cyber threats requires close collaboration among a wide range of stakeholders—including utility companies, equipment and technology vendors, regulatory agencies, and researchers at national laboratories and universities.

These stakeholders already have made substantial progress toward characterizing and tracking cyber risks, and public-private partnerships are working to address these risks. As the industry develops and implements smart grid systems across multiple utility domains, continued commitment will be critical for mitigating immediate threats, while also planning for the long-term requirements of a modernized electric grid.

Public-Private Security Efforts

The release of the 2006 *Roadmap to Secure Control Systems in the Energy Sector*—facilitated jointly by the U.S. Department of Energy and the Department of Homeland Security—established a public-private partnership to enhance cyber security in the energy sector. The Roadmap provides a common vision and collective plan to improve cyber security over 10 years, through systems assessment, next-generation R&D, best practices, and outreach. Because the Roadmap was built on the collective insights of the control systems community—including owners and operators, commercial vendors, national laboratories, industry associations, and government agencies—it helped launch a host of projects and initiatives. A user-driven online tool, the interactive energy Roadmap[1] (ieRoadmap), is tracking the progress of more than 65 projects linked to specific Roadmap goals.

In 2010, industry began updating the Roadmap to address emerging smart grid cyber security considerations and the evolving technology and changing threat landscape of the energy sector. This update, the 2011 draft *Roadmap to Achieve Energy Delivery Systems Cybersecurity*,[2] outlines strategies and milestones that aim to enable industry and government to design, install, operate, and maintain resilient energy delivery systems that will survive a cyber incident while sustaining critical functions. Multiple government agencies and industry organizations are using the Roadmap to allocate resources and support a number of activities that directly align with the Roadmap goals *(see sidebar, "Collaborating on Cyber Security")*.

Continued commitment is critical for mitigating immediate threats, while also planning for the long-term requirements of a modernized grid.

With $12 million of financial assistance through the *American Recovery and Reinvestment Act* (ARRA), DOE's Office of Electricity Delivery and Energy Reliability (OE) is collaborating with NIST and industry organizations to continue developing a framework and roadmap for interoperability standards, while ensuring cyber security is a key consideration[3] *(see sidebar, "NIST 7628: Framework for Progress")*. OE is also partnering with a consortium of leading utilities to support ASAP-SG in developing a set of vendor-neutral security profiles that provide baseline security controls for a given smart grid application. Four security profiles have been completed, offering guidelines for securing advanced metering infrastructure (AMI), third-party data access, distribution management systems and most recently, wide-area monitoring, protection, and control applications (*i.e.*, synchrophasors). Each profile defines a scoping boundary and provides a reference architecture including a set of use cases, a failure analysis, and a set of required controls specifically applied to devices and components according to their functional responsibilities.

Most recently, DOE announced a public-private investment of $16.5 million to form the National Electric Sector Cybersecurity Organization (NESCO) to help improve electric system reli-

---

Henry S. (Hank) Kenchington is deputy assistant secretary at the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability. **Carol Hawk** is a program manager in the office. **Darren R. Highfill** is founder of UtiliSec, an independent utility security consultancy. **Jack Eisenhauer** is president and CEO of consulting firm Nexight Group LLC, and **Lindsay Kishter** is a communications specialist with the firm.

This is the second of a two-part article edited from the authors' report, *Cyber Security for the Smart Grid*, scheduled for publication on Fortnightly.com (www.fortnightly.com/whitepapers.cfm). The first part was published in Fortnightly's July 2011 issue.

NIST 7628: Framework for Progress

At the national level, the *Energy Independence and Security Act* of 2007[1] assigned NIST the primary responsibility to coordinate the development of a framework for protocols and standards to achieve interoperability of smart grid devices and systems.[2] NIST's *Framework and Roadmap for Smart Grid Interoperability Standards-Release 1.0*[3] describes a reference model for the smart grid and identifies 75 applicable existing standards and 15 high-priority gaps.

As a part of that larger effort, NIST established a Cyber Security Working Group (CSWG) under its 450-member public-private Smart Grid Interoperability Panel (SGIP) to develop the NIST Interagency Report (IR) 7628: *Guidelines for Smart Grid Cyber Security*.[4] This document provides a common starting point and framework for the smart grid's high-level security architecture. NIST IR 7628 can be used to examine overall system risk and determine high-level security requirements for smart grid applications by following a methodical approach guided by the diagrams, tables, and data in the document. A utility can use NIST IR 7628 to link security requirements for a smart grid application to the utility's overall smart grid strategy and security posture. Ultimately the document serves as an industry-wide reference that the utility may use as a starting point to drive deeper in their analysis and determine security requirements for the specific smart grid application they wish to implement.–***HK* et al.**

Endnotes

1. *Energy Independence and Security Act* of 2007, Public Law 110–140, 110th Cong., 1st sess., Dec. 19, 2007.
2. National Institute of Standards and Technology, "Smart Grid," last updated Feb. 16, 2011.
3. National Institute of Standards and Technology, *Framework and Roadmap for Smart Grid Interoperability Standards*, Release 1.0, Special Publication 1108, NIST, January 2010.
4. National Institute of Standards and Technology (NIST), *Guidelines for Smart Grid Cyber Security*, NIST Interagency Report 7628, NIST, August 2010.

ability by supplying data analysis and forensics capabilities for cyber-related threats. Led by the Energy Sector Security Consortium Inc. (EnergySec), it also is creating a framework to share information, best practices, resources, and solutions among domestic and international electric sector participants. Funding also supports the development of NESCOR, the National Electric Sector Cybersecurity Organization Resource, which is led by EPRI and conducts assessment and analysis of cyber security requirements, results, and standards in addition to testing security technologies in labs and pilot projects in support of NESCO.

These (and others described in the sidebar "Collaborating on Cyber Security") represent only a selected handful of the many ongoing collaborative efforts that combine industry leadership and public support to advance cyber security R&D specifically for future smart grid applications.

Cyber Security in ARRA Investments

In November 2009, Congress placed greater emphasis on a nationwide plan to modernize the electric power grid, enhance the security of U.S. energy infrastructure, and promote reliable electricity delivery. Through ARRA, Congress provided DOE with $4.5 billion to jumpstart grid modernization through smart grid programs previously authorized by the *Energy Independence and Security Act* of 2007 (EISA). DOE leveraged the ARRA funding to create a public-private investment opportunity worth a total of more than $10.3 billion ($4.5 billion of DOE funds leveraged with $5.8 billion of private sector funds). Most of this funding supports implementation of 131 grants and projects across the country.[4]

Each project recipient committed to implement a cyber security plan that includes an evaluation of cyber risks and planned mitigations, cyber security criteria for device and vendor selection, and relevant standards or best practices the project will follow. The cyber security plans must address the following points:

- How cyber security risks will be mitigated;
- What criteria will be used for vendor and technology selection;
- The relevant cyber security standards that will be followed (or in the absence of standards, what industry best practices will be used); and
- How emerging smart grid cyber security standards that are currently being developed can be implemented in the future deployment life cycle.

By using established standards and best practices, recipients avoid the need to re-engineer security from the ground up.

Specifically, recipients must be able to illustrate the ability to accomplish these objectives: maintain capability for timely detection and response; mitigate the consequences of a cyber event; correct exploited vulnerabilities; and restore affected systems, networks, and equipment.

DOE asks recipients to map each objective across the project life cycle and show plans for how each objective will be addressed along the way. DOE encourages recipients to draw upon methods using NIST Interagency Report 7628: *Guidelines for Smart Grid Cyber Security*, ASAP-SG Security Profiles, and the suite of national and international standards and specifications. By doing so, recipients avoid the need to re-engineer security requirements from the ground up, while aligning themselves with industry best practices, and providing DOE and other

stakeholders with a strong basis for project evaluation.

To help project leaders develop and implement their cyber security plans, DOE created a website—www.arrasmartgridcyber.net—that aids participants in sharing best practices. The DOE is producing a set of outreach webinars to engage project recipients. The first of these webinars was presented in February 2011, and DOE expects to perform several more throughout the duration of the project to guide projects as they mature. The webinars aim to provide tangible guidance in applying this framework to real-world projects to implement best-practice cyber security measures.

Securing the Future

Integrating information technology and digital communications systems is essential to building the smart grid and realizing its benefits. New technologies, components, capabilities, and stakeholders will deliver untold operational advances and help the electricity industry manage a variety of new risks—but only if industry designs security into new components and integrates them safely with legacy systems.

The increasing complexity, scale, and interconnectedness of the North American electricity system make its protection and resilience a shared public-private responsibility. This is a key principle of a new report, *A Policy Framework for a 21st Century Grid: Enabling Our Secure Energy Future*,[5] issued by the President's National Science and Technology Council. It recognizes the need for sustained cooperation among the private sector, state and local governments, the federal government, consumer groups, and other stakeholders to realize smart grid benefits. The *Policy Framework* calls for continued investment in research, development, and demonstration; strong information sharing from smart grid deployments; better protection and empowerment of consumers; and a sound regulatory framework at the state and federal level. To ensure a secure grid, it endeavors to have the federal government facilitate the development of rigorous, open standards and guidelines for cybersecurity through public-private cooperation; and to work with stakeholders to promote a rigorous, performance-based cybersecurity culture, including active risk management, performance evaluations, and ongoing monitoring.

To improve smart grid security and address emerging needs and gaps, a multi-faceted approach will be needed that draws upon the specialized capabilities, knowledge, and economic resources of key stakeholders. The following steps can ensure these capabilities and resources are properly leveraged for this purpose.

1) *Develop advanced technologies to create a resilient electricity infrastructure:* The newly revised *Roadmap to Achieve Energy Delivery Systems Cybersecurity* provides a plan for organizing and leveraging public and private capabilities and resources to develop advanced cyber security technologies that respect the unique design and operating constraints of energy delivery systems and can provide the end-to-end security needed for a modern and resilient electricity system. Achieving the Roadmap goals will require continued collaboration among government and industry partners to pursue activities that are aligned with the Roadmap's vision and aimed at creating a resilient infrastructure. As new technologies or capabilities are introduced, this partnership must encourage a thorough and continuous examination of potential cyber vulnerabilities. The electric sector's growing culture of security should support a graded risk management approach for implementing new technologies that appropriately balances the benefits of the capability with its potential risks.

Data protection laws offer some privacy protection, but the smart grid introduces a new use of private information.

2) *Encourage industry to share and adopt best practices:* The early implementation of smart grid technologies has begun to uncover good practices for cyber security that improve interoperability, reliability, resilience, efficiency, and security across all phases of the technology life cycle. Industry and government can work together to formally define best practices in designing, implementing, and using smart grid technologies, and widely share that information through workshops, public-private partnerships, and education programs. This will enable all stakeholders to access user-friendly, actionable best practice information as it becomes available.

3) *Build a dynamic security posture to address evolving threats:* Changing and evolving threat profiles require flexible and dynamic approaches and technologies to continually enhance both the physical and cyber security posture of the electricity infrastructure. As the threat landscape continually evolves, security posture must adapt and be able to rapidly respond to incidents and new threat information. The goal is to deliver a speedy response to new information without affecting the core functionality and reliable operation of the infrastructure.

Industry and government should work together to continually monitor the threat landscape and integrate or upgrade physical and cyber security safeguards as new technologies are introduced and adversary capabilities evolve. All electric utilities, other electric service providers, microgrids, consumer systems, area operating centers, and regional coordinators must be included in this ongoing threat assessment, which should include new methods and procedures to exchange or distribute threat information.

4) *Build a coordinated regulatory framework:* Today's patch-

Collaborating on Cyber Security

The U.S. Department of Energy's (DOE) Cybersecurity for Energy Delivery System program is funding research, development, and demonstration projects led by industry, academia, and national laboratories. As part of this effort, the widely recognized control system vulnerability assessments conducted at the DOE National SCADA Test Bed (NSTB) have helped industry identify and mitigate vulnerabilities, and develop more secure SCADA systems that are now being deployed in the energy sector. Continuing assessments on systems now in the marketplace and new smart components will build on the test bed's lessons learned, which it publishes in a regular *Common Cyber Security Vulnerabilities Assessment* report[1] for utilities and vendors to use in securing these systems.

Vendors, researchers, and infrastructure owners and operators (including utilities) are working closely with the government on a robust portfolio of R&D aimed at developing the next generation of systems and components for the smart grid. The Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) research program, built on a National Science Foundation initiative, is a consortium of five universities that is working at the intersection of power system engineering and the computer science of cyber security to research and develop next-generation cyber security capabilities tailored to the unique design and operational constraints of energy delivery systems—such as real-time availability, integrity, authentication, and confidentiality of SCADA command and control communications—that are key to a modern, reliable, and efficient electric power grid. Funded by DOE and DHS, the five-year effort is working on a range of activities to build trusted systems from untrusted components, secure low-level devices, communications, and data systems to ensure trustworthy grid operation during normal conditions, cyber attacks, and power emergencies.

The DHS National Cyber Security Division (NCSD) has also launched the Industrial Control System Computer Emergency Response Team (ICS-CERT), which shares information on threats and vulnerabilities to control systems and deploys incident response teams to investigate and help correct cyber incidents and attacks. DHS conducts advanced control systems security training and publishes best practices and recommendations to enhance cyber security for control systems across all critical infrastructure sectors, such as the *Primer Control Systems Cyber Security Framework and Technical Metrics*.[2] Its Control Systems Security Program also supports the Industrial Control Systems Joint Working Group (ICSJWG), which encourages public-private communication and partnership on security issues across all critical infrastructures in the United States.

The DHS Science and Technology Directorate is funding DETECT, a project designed to create an isolated, 400-node miniature Internet that cyber security researchers can use to investigate malware and other security threats without danger of infecting the real Internet. Run out of the DETERlab (for Cyber Defense Technology Experimental Research) at the University of Southern California, part of the project aims to build a community of researchers using the DETERlab platform to crowd-source cyber security solutions and improve information sharing among researchers.[3] All of these activities support the cyber security of a modern, digital electricity infrastructure as a key objective of national smart grid efforts.–***HK* et al.**

Endnotes

1. U.S. Department of Energy National SCADA Test Bed, *Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program*, Idaho National Laboratory, November 2008.
2. Department of Homeland Security Control Systems Security Program, National Cyber Security Division, *Primer Control Systems Cyber Security Framework and Technical Metrics*, DHS, June 2009.
3. Rowinski, Dan, "DHS backs mini-Internet test bed for cybersecurity," *Government Computer News*, Jan. 18, 2011.

work of standards and regulations exists to address various aspects of the nation's electricity system. No single regulatory authority addresses all aspects of the nation's electricity infrastructure; jurisdictional boundaries include distinctions between state and federal regulatory authority, ownership differences between public and private power utilities, and the international connections with Canada and Mexico. State and federal regulators need to work together to implement comprehensive, end-to-end regulations to address smart grid issues common to both interstate bulk power transmission and localized distribution systems.

5) *Address customer energy usage data sharing and privacy concerns:* Smart grid technologies will greatly expand the amount of consumer data that can be monitored, collected, aggregated, and analyzed, which has raised privacy concerns. As smart grid capabilities are deployed, the need to protect consumer data and educate customers on privacy risks and mitigations will remain a central focus of cybersecurity efforts. Volume 2 of NIST Interagency Report 7628: *Guidelines for Smart Grid Cyber Security* identifies many of the smart grid challenges with data sharing and privacy issues and provides a starting point to address them.

Existing data protection laws and regulations offer some privacy protection, but the smart grid introduces a new use of private information that current policy might not adequately address. New guidelines and regulations are needed to inform the privacy practices and policies of smart grid stakeholders and give consumers confidence that their data is being properly used and protected. Federal, state, and local regulators must work with industry to develop policy frameworks for sharing data in a manner that is secure, protects privacy, and addresses other

information sensitivities.

6) *Develop secure interoperability standards:* Numerous utilities, third-party services, and other stakeholders will be deploying large numbers of intelligent devices and systems, with the expectation that they will easily and reliably integrate and operate together across the grid. By designing and building to interoperability standards, vendors can ensure their systems and components will integrate with those from other vendors. Industry organizations continue to work with numerous government organizations to develop interoperability, wireless, and other standards that will ensure higher security and reliability of smart grid components. Industry and government should continue working to refine and develop standards that enable responsiveness to rapidly evolving threats and technologies.

7) *Promote open information sharing between industry and government:* The limited exchange of threat, vulnerability, and incident information can prevent the sector from building the business case necessary to increase private investment in cyber security. Stakeholders also need credible, actionable, and timely information to prepare for potential threats and rapidly mitigate power systems vulnerabilities before they are exploited. Government and industry should work together to build a secure forum for information exchange that brings the right people to the table and clarifies roles and responsibilities. The forum should enable information sharing to and from government, but also among owners and operators. This will give each stakeholder the confidence and a clear mechanism to share information that could be critical to others. The government must also work with industry to establish a legal framework for effective information sharing that addresses the regulatory, privacy, or pricing sensitivity issues that create legal barriers or disincentives for vulnerability and incident disclosure.

Smart grid technologies promise to deliver a grid that is more reliable and resilient, and able to more readily withstand and recover from malicious and natural acts. As government, industry, and academia work to develop advanced technologies and new cyber controls, they have the opportunity to get security right by building an infrastructure that thoroughly addresses cyber needs in every component. Continued commitment by the private and public sector will be needed to mitigate immediate issues in the short term and address the long-term needs of a smarter grid. F

Endnotes:

1. U.S. Department of Energy, "interactive energy Roadmap." http://www.controlsystemsroadmap.net/
2. *Roadmap to Achieve Energy Delivery System Cybersecurity,* U.S. Department of Energy, 2011.
3. National Institute of Standards and Technology, "Smart Grid," last updated Feb. 16, 2011.
4. See smartgrid.gov for full details on the DOE Smart Grid Investment Grant and Smart Grid Demonstration Project programs, including impact and benefit analyses.
5. National Science and Technology Council, *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future*, The White House, June 13, 2011.