

MARCH 2007

TRANSMISSION & DISTRIBUTION WORLD

TM

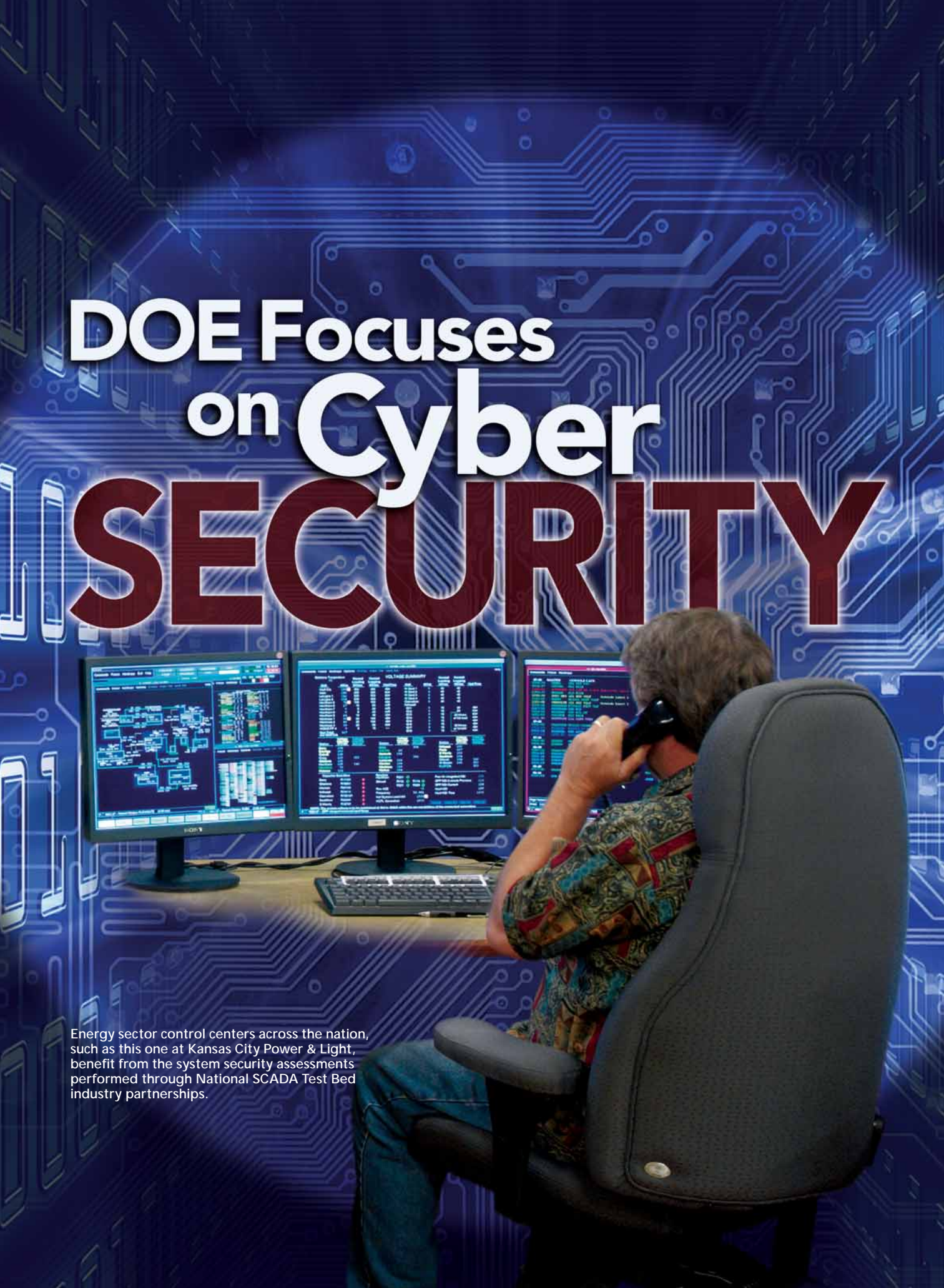
www.tdworld.com

A PENTON MEDIA PUBLICATION

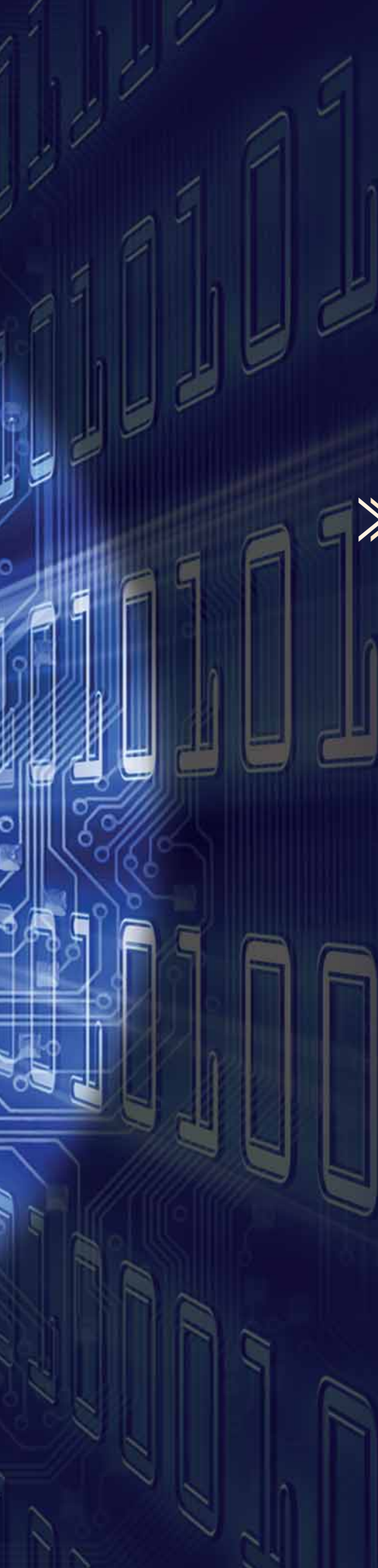
Cyber SECURITY



DOE Focuses on Cyber SECURITY



Energy sector control centers across the nation, such as this one at Kansas City Power & Light, benefit from the system security assessments performed through National SCADA Test Bed industry partnerships.



Energy sector owners, operators and system vendors team up to boost control system security with National SCADA Test Bed.

By Matt Tani, *Automation Editor*

THE POTENTIAL FOR VULNERABILITIES IN THE ELECTRONIC SYSTEMS THAT MONITOR AND CONTROL OUR ENERGY INFRASTRUCTURE has increased steadily since the mid-1990s. As control systems became increasingly interconnected with other control and corporate data networks, the potential for cyber intrusion grew as well. When the U.S. Department of Energy (DOE) established the National SCADA [supervisory control and data acquisition] Test Bed (NSTB) in 2003, it initiated a voluntary partnership among U.S. energy sector owners and operators, system vendors and the federal government. This public-private partnership is actively improving cyber security in the electronic systems that control the flow of electric energy in the United States.

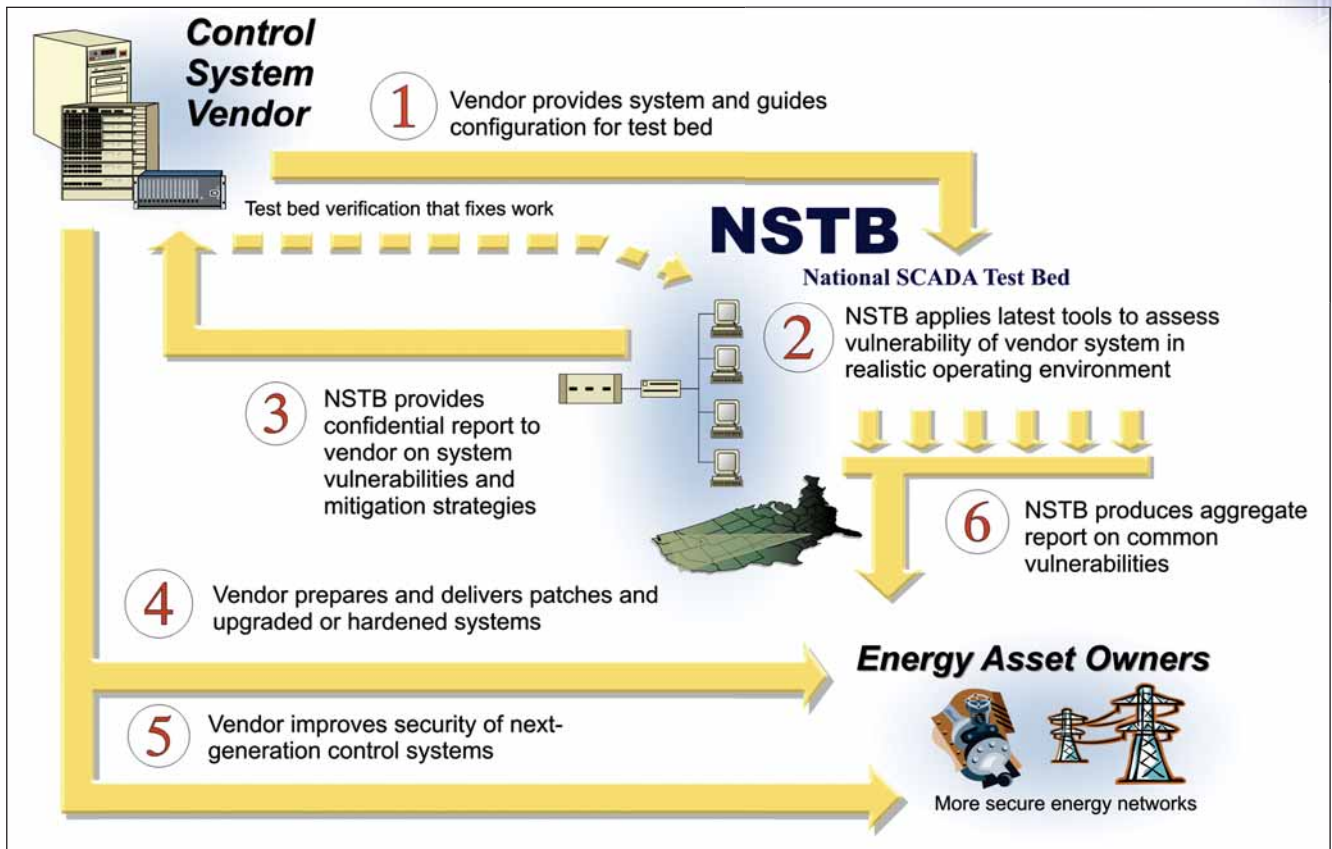
This voluntary collaboration has been a resounding success thanks to the strong leadership and follow-through by the U.S. energy asset owners and operators, the willing participation of forward-thinking control system vendors and the specialized resources of the DOE laboratories in the NSTB. Vendors representing more than 80% of the new SCADA systems entering U.S. energy markets are now participating in this proactive partnership.

Collectively, members of the NSTB partnership are continuously expanding the energy sector's knowledge, methodologies and technologies for protecting control systems in today's evolving threat environment. Specifically, the NSTB control system assessments have strengthened security profiles for both new and existing systems. Owners and operators have earned high marks for quickly implementing upgrades and software patches supplied by their system vendors. Leading vendor participants now include ABB (Zurich, Switzerland), AREVA (Paris, France), GE Energy (Atlanta, Georgia, U.S.), Open Systems International (Minneapolis, Minnesota, U.S.), Siemens (Erlangen, Germany) and Telvent (Madrid, Spain).

THE COLLABORATION

The DOE's Office of Electricity Delivery and Energy Reliability (OE) conceived the NSTB as a specialized multilaboratory resource to enhance control system security by working directly with vendors, owners and operators of U.S. electricity, oil and natural gas systems. "The NSTB fills a critical need," said OE Director Kevin Kolevar. "We are listening to industry and responding. Only by government and industry working together can we tackle the tough cyber security challenges facing the energy sector."

The NSTB effort is part of a much larger collaboration between government and the energy sector to improve control systems security. In 2005, the DOE collaborated with energy sector leaders to develop the "Roadmap to Secure Control Systems in the Energy Sector." This landmark document presents an industry-defined vision, and near- and long-term requirements for protecting all energy control systems from losing critical function due to intentional cyber assault within the next



Enhancing the security of energy control systems today.

10 years. The Critical Infrastructure Protection Committee of the North American Electric Reliability Council (NERC) unanimously endorsed the Roadmap document, which recognizes the need to maintain the NSTB to work with vendors and asset owners to test equipment, architectures and processes.

The NSTB is funded by the DOE and jointly managed by the Idaho National Laboratory (INL) and Sandia National Laboratories (SNL), drawing upon specialized expertise from the Argonne, Oak Ridge and Pacific Northwest national laboratories. A key element of the NSTB effort is a highly effective process for assessing the security of current control systems in a realistically simulated, yet controlled and protected environment. At first, though, the partnership faced many uncertainties:

- Would control system vendors be willing to work with NSTB on the assessments?
- Would system vendors act promptly to address any vulnerabilities identified during the assessments?
- Would utilities and other system owners recognize the business value of increased security?
- Would owners and operators be willing to devote resources to applying the resulting system patches and upgrades in the diverse control systems currently in use?

All of these questions have been emphatically answered in the affirmative. Why are utilities embracing the NSTB program? Tom Glock, manager of power operations at Arizona Public Service Co. (APS; Phoenix, Arizona, U.S.), said,

“APS is developing a new EMS [energy management system], scheduled to be in production the third quarter of 2007. The security of our energy control system is critical to our mission of providing safe, reliable electric service to our customers. APS welcomed the opportunity to work with the DOE and our vendor to verify that our EMS remains secure. We believe the security of our EMS directly relates to our electric system reliability.”

System vendors are similarly enthusiastic. According to Neela Mayur, product manager for ABB Inc., her company saw immediate value in the partnership. “ABB recognized that NSTB offered an excellent opportunity to get cyber security experts involved in validating and improving system security features,” she said. “We’re pleased to have been the first to partner with NSTB.”

By undergoing the NSTB assessment process, industry leaders have taken a proactive stance against cyber intruders. Vendors have worked with NSTB on a 50/50 cost-shared basis to assess their systems and are implementing NSTB recommendations, as needed, to deliver effective system fixes to their customers. End users in the energy sector have been similarly prompt in applying the security fixes, patches, upgrades and guidance provided by vendors and NSTB.

THE PROCESS

When a system vendor initially seeks NSTB testing of its product, company representatives typically meet with NSTB experts from the INL to discuss and develop a formal Cooperative



Control system vendors invest considerable resources so that NSTB experts can challenge their security defenses.

Research and Development Agreement (CRADA) and test plan. Once the necessary legal reviews and signatures are obtained, the vendor works with NSTB to deliver and guide the secure installation of one of its current commercial systems at the lab.

Using the test plan and selected targets of evaluation, the NSTB cyber security experts apply the latest exploit tools and techniques to try to hack into the control system. These rigorous attacks thoroughly test the system for potential vulnerabilities that might be exploited in a cyber attack.

After testing, the NSTB provides the vendor a detailed and highly confidential report on the findings of the SCADA assessment. Each report recommends approaches or strategies for correcting any identified vulnerabilities. Although vendors are not bound to act on these findings or recommendations, they are expected to use their discretion in developing system patches, upgrades or customer updates. This trust has not been misplaced. Participating vendors that have completed the entire assessment process have acted promptly in implementing NSTB recommendations and sharing results with utility customers; other participating vendors are expected to follow a similar course.

According to Ron Larson, manager of strategic technologies and growth initiatives at GE Energy, "NSTB activities provide a vital starting point by uncovering inherent vulner-

abilities in the standard product offerings of major control system vendors. Vendors that participate in the assessments gain a much clearer understanding of any security issues in their standard product, which then helps them better secure the control systems that operate critical national infrastructures."

After incorporating suggested security fixes into a product, the system vendor typically sends it to NSTB for testing and validation. Once completed, the NSTB submits a final Cyber Security System Test Report to the vendor and presents the findings to vendor management and technical staff. The vendor decides on the best channels for disseminating the system patches or upgrades to existing customers in the energy sector.

Vendors also incorporate their new knowledge and security strategies into new products under development. Though this process requires significant investment by both vendors and asset owners, industry feedback clearly indicates that the security benefits justify the costs.

Brent Brobak, senior product manager for security and SCADA at AREVA T&D Automation, said, "The program has been a real learning experience for AREVA and worth every dollar we invested. AREVA products now in use by many North American utilities have been hardened against external cyber attacks as a direct result of our NSTB assessment."

Paul Skare of Siemens PTD Inc. commented on the larger picture: "Siemens has found that the awareness and training that occur in both directions as a part of the assessment process are beneficial. The methodologies in use at the NSTB, combined with the assessment reports, provide valuable insight into control system security — and the entire industry benefits."

Through these system assessments, NSTB experts have expanded their knowledge and understanding of potential control system weaknesses and the best ways to mitigate them. NSTB uses this acquired expertise to assemble "common vulnerabilities" reports to help owners and operators understand their exposure and how to take effective remedial action. In addition, more than 1000 end users have attended NSTB training to learn more about vulnerabilities and protective measures. The NSTB team also offers traveling simulations of cyber attacks and remediation strategies to enhance understanding of system weaknesses and workable solutions.

THE SUCCESSES

Some vendors have been willing to share details of their assessments through presentations at user group meetings, and some have shared the detailed NSTB test reports directly with their users. This information sharing helps asset owners and operators determine the most appropriate approach to reduce any vulnerabilities in their specific systems.

According to Mark Baustert, chair of the ABB Network Manager Users Group, "NSTB assessment results shared through the ABB EMS user group meetings have helped users gain a better understanding of their network vulnerabilities. Many utilities have now applied this knowledge to easily reduce certain vulnerabilities."

Although many successes tend to be anecdotal because of the need to protect sensitive assessment results, the NSTB partnership is unquestionably strengthening the security of energy control systems — both new and previously deployed. Each control system tested by the NSTB to date represents a large share of new SCADA systems entering the energy sector, and security benefits continue to expand as these improved systems move into wider use. In addition, each weakness that is found and fixed can benefit legacy systems with similar vulnerabilities. One of the six participating vendors reported 14 security-enhanced systems now in active operation, while another reported at least 49 security patches downloaded by major utility customers.

The ongoing success of the NSTB partnership results from several of its unique features:

- System vendors know the NSTB team respects the sensitivity of their system information and will actively protect it.
- Vendors are not obligated to take specific actions in response to assessment findings, but are expected to act in good faith to serve their customers.
- The DOE national laboratories on the NSTB team share and leverage their expertise to produce a widening ripple of awareness, knowledge and other benefits.
- Asset owners and operators were quick to recognize the risks and many are now actively pushing for stronger security measures.

Often, vendors and asset owners and operators can substantially improve control system security by simply making better use of existing capabilities in deployed systems. Examples include fully patching operating systems, improving password management practices and implementing layered security defenses. However, users are not always aware that these features exist. “We had to educate our clients a little bit better on what features were in there that were native to the

product,” noted Al Rivero of Telvent. “Everything from strong authentication passwords, active directory rules, areas of responsibility — those now come out of the box.”

THE FUTURE

Cyber threats continue to evolve and the tools to hack into critical systems are becoming more sophisticated. The NSTB collaboration represents an ongoing effort to keep control system security a step or two ahead of this dynamic threat. The continuing need for assessments, advanced technology research, outreach, training and standards development are all reinforced by the Roadmap document. The DOE laboratories on the NSTB team are currently pursuing activities in all of these areas in partnership with industry.

What’s ahead? DOE labs are developing advanced technology that will enable more secure control systems in the future. For example, SNL is leading efforts to develop a modeling and simulation tool that industry can use to analyze the security of large control systems, and the Pacific Northwest National Laboratory is developing a novel technology for authenticating clear text SCADA communications.

Asset owners and operators across the energy industry are becoming more aware of cyber risks to their control systems and many are taking the initiative to improve security. Several utilities have expressed interest in NSTB field assessments to verify the effectiveness of security upgrades in deployed systems. The first such NSTB field assessments are now in progress — one more example of the widening circle of benefits from the NSTB partnership. Despite progressive security improvements achieved through the NSTB, Mayur warns against complacency. “This is not a one-shot process, and there’s no such thing as a completely secure system,” she said. “We must continue our vigilance and keep raising the bar against the escalating threat of cyber intrusion.” **TDW**

Reprinted with permission from the March 2007 issue of *Transmission & Distribution World*® (www.tdworld.com)
Copyright 2007, Penton Business Media. All rights reserved.

TD-154-EKK

**For more information
about NSTB, contact:**

**Hank Kenchington,
Program Manager
Control Systems Security**

208-526-1878

Henry.Kenchington@hq.doe.gov



U.S. Department of Energy

Office of Electricity Delivery & Energy Reliability

Research and Development, Cyber Security Systems

www.oe.energy.gov/randd/css.htm